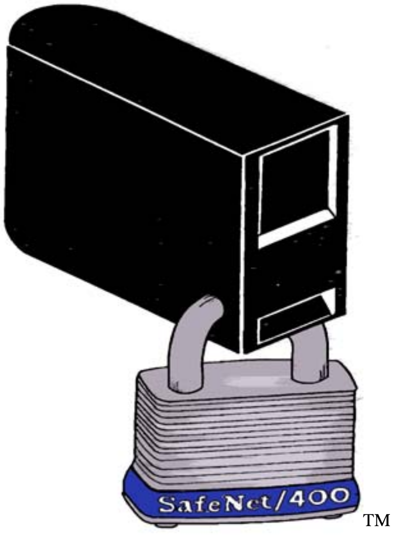
SAFENET/400

REFERENCE GUIDE

Version 8.50



How to contact us

Direct all inquiries to:

Kisco Information Systems
89 Church Street
Saranac Lake, New York 12983

Phone:	(518) 897-5002
Fax:	(518) 897-5003

SafeNet/400 Website:	http://www.kisco.com/safenet
SafeNet/400 Support Website:	http://www.kisco.com/safenet/support

Visit the SafeNet/400 Web Site at HTTP://WWW.KISCO.COM/SAFENET

TABLE OF CONTENTS

SafeNet/400
Reference Guide

Chapter 1 - SETTING UP USERS

Navigating through the screens

You can perform each of the steps outlined in this chapter by using the corresponding option on the SafeNet/400 Main Menu. However, if you are setting up a new user, when you are finished with one screen you can use **F9** to advance to the next without returning to the main menu. If you want to skip a step, you can cancel and return to the SafeNet/400 Main Menu.

Group Profiles

If you have an unlimited user license for **SafeNet/400**, Group Profiles are available. If so, you may use **F7** to toggle between the group profile settings and the user profile settings.

F8 will display all the user profiles within the group.

Setting the User Logging Levels

The valid logging levels are:

Logging Level A	Log all transactions
Logging Level R	Log only rejected requests
Logging Level N	No logging

As you set up your user logging levels, please keep in mind the following:

- If you set the logging level on the Server Function (WRKSRV) to *NO LOGGING* or *REJECTIONS*, the Server Function (WRKSRV) setting will override the individual user logging level.

- If you set the logging level on the Server Function to *ALL*, the individual user logging level will override the Server Function logging level.

To make sure you are logging transactions correctly, we recommend that when you initially set up **SafeNet/400** you set the Server Functions to log *ALL* and set the User to Server logging levels to either *ALL* or *REJECTIONS*.

Then, after you have had some experience with checking the logs and interpreting the results, you may want to make changes for specific user and server combinations.

An example of this might include certain "trusted" user profiles. If you trust the user in question and are concerned about the size and amount of logging activity, you might choose to only record rejected transactions for that user.

Another example might be a known client server application that is clearly defined and does not need to be monitored. For these applications you might choose to stop logging altogether. We have found several fax applications that fall into this category. They generate a large number of entries that are really not needed for your purposes in controlling access security.

SafeNet Administrator

You can set up a SafeNet/400 Administrator, or 'Super Admin' from the SafeNet/400 Special Jobs Menu or by using the WRKSNADM command. This can also be found on the Special Jobs Menu, **Option 5 – Maintain SafeNet Administrators**.

The WRKSNADM command can be executed by a user with *SECADM or *SECOFR authority.

A user profile must be set up as a SafeNet/400 'Super Admin' to perform the following:

Activate or deactivate SafeNet/400
Change/copy/remove the IBM-supplied Q profiles settings in SafeNet/400
Use the WRKSRV, CHGSPCSET, CHGFTPSET commands

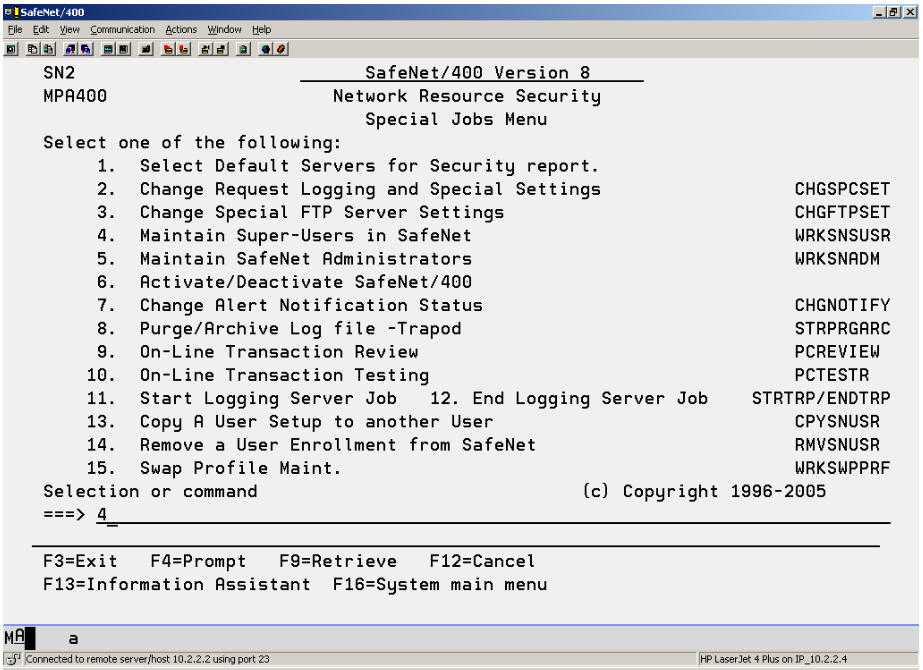
A regular SafeNet/400 user or administrator does not have authority to the above functions.

Unless specifically changed, QSECOFR is ALWAYS a SafeNet/400 Super Admin. User profile SAFENET is a Super Admin; this status can be changed or removed to suit your purposes.

Super Trusted User Control

Under special circumstances it may be necessary to have a user that should not be checked through all the **SafeNet/400** security routines. Transactions from these users can bypass the traditional **SafeNet/400** security routines; you can choose to simply log them or not log them.

From the <u>Special Jobs Menu</u> select **Option 4 – Maintain Super-Users in SafeNet**.



```
   SN2                          SafeNet/400 Version 8
   MPA400                    Network Resource Security
                                Special Jobs Menu
   Select one of the following:
        1.  Select Default Servers for Security report.
        2.  Change Request Logging and Special Settings             CHGSPCSET
        3.  Change Special FTP Server Settings                      CHGFTPSET
        4.  Maintain Super-Users in SafeNet                         WRKSNSUSR
        5.  Maintain SafeNet Administrators                         WRKSNADM
        6.  Activate/Deactivate SafeNet/400
        7.  Change Alert Notification Status                        CHGNOTIFY
        8.  Purge/Archive Log file -Trapod                          STRPRGARC
        9.  On-Line Transaction Review                              PCREVIEW
       10.  On-Line Transaction Testing                             PCTESTR
       11.  Start Logging Server Job   12. End Logging Server Job    STRTRP/ENDTRP
       13.  Copy A User Setup to another User                       CPYSNUSR
       14.  Remove a User Enrollment from SafeNet                   RMVSNUSR
       15.  Swap Profile Maint.                                     WRKSWPPRF
   Selection or command                         (c) Copyright 1996-2005
   ===> 4

   F3=Exit   F4=Prompt   F9=Retrieve   F12=Cancel
   F13=Information Assistant  F16=System main menu

MA     a
```

Connected to remote server/host 10.2.2.2 using port 23 HP LaserJet 4 Plus on IP_10.2.2.4

You can turn logging on or off for Super Trusted Users by using the CHGSPCSET command and changing the LOGUSER parameter to *YES or *NO.

Note: This should only be used under conditions when you want **NONE** of the specified users transactions to be checked through **SafeNet/400** security routines.

Entering User Security Levels

If you plan on setting any of the Server Functions to Level 3 or Level 4, and anticipate doing anything other than simply logging all requests, the first step in configuring **SafeNet/400** is to give the users authority to any Server Functions they require.

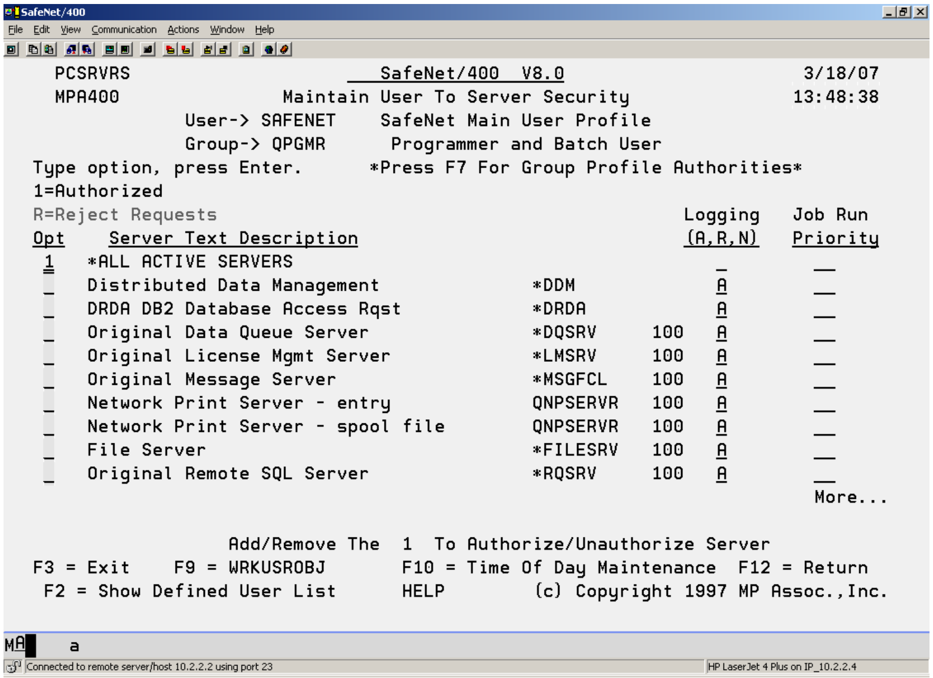
1. From the SafeNet/400 Main Menu select **Option 2 - Work with User to Server Security** or use **WRKUSRSRV** command

   The *Work User to Server Security Enter User Profile* screen appears.

2. **Type the user profile** you will be setting up, or ***PUBLIC**, then **ENTER.**

   If you would like a list of all user profiles on the system, press **F4** or type ***ALL.**

   To see a list of users already defined within **SafeNet/400** type ***ALLDFN**.



```
    PCSRVRS                         SafeNet/400  V8.0                     3/18/07
    MPA400                Maintain User To Server Security                13:48:38
                User-> SAFENET     SafeNet Main User Profile
                Group-> QPGMR       Programmer and Batch User
  Type option, press Enter.     *Press F7 For Group Profile Authorities*
  1=Authorized
  R=Reject Requests                                           Logging   Job Run
  Opt    Server Text Description                              (A,R,N)   Priority
   1    *ALL ACTIVE SERVERS                                      _        __
   _    Distributed Data Management            *DDM              A        __
   _    DRDA DB2 Database Access Rqst          *DRDA             A        __
   _    Original Data Queue Server             *DQSRV     100    A        __
   _    Original License Mgmt Server           *LMSRV     100    A        __
   _    Original Message Server                *MSGFCL    100    A        __
   _    Network Print Server - entry           QNPSERVR   100    A        __
   _    Network Print Server - spool file      QNPSERVR   100    A        __
   _    File Server                            *FILESRV   100    A        __
   _    Original Remote SQL Server             *RQSRV     100    A        __
                                                                         More...

                    Add/Remove The  1  To Authorize/Unauthorize Server
  F3 = Exit    F9 = WRKUSROBJ       F10 = Time Of Day Maintenance  F12 = Return
   F2 = Show Defined User List      HELP        (c) Copyright 1997 MP Assoc.,Inc.

MA     a
```

Connected to remote server/host 10.2.2.2 using port 23
HP LaserJet 4 Plus on IP_10.2.2.4

   The *Maintain User to Server Security* screen appears.

   A list of all the servers is displayed.

3. If you would like to see the list of all users who have been defined within **SafeNet/400**, press **F2.**

Type 1 in the *Option* column in front of each server this user will have access to.

If they will have access to all the server functions, **select**

***ALL ACTIVE SERVERS**

To remove access to a particular server, remove the '1' and leave the *Option* column blank for that server.

4. **Enter** the *Logging Level* for each server.

   A = All
   R = Rejections only
   N = No logging

   When you have finished setting up servers for this user, press **ENTER.**

5. Enter the *Job Run Priority* for each server. Do this if you choose to override OS/400 job priority defaults.

   The job priority will be set when the user accesses this server. Valid job priorities are 00 (the default) through 99. A value of 00 indicates no change to the default job priority.

6. **Press F9** to continue to the next step - setting up user authorities to objects.

Entering User Authorities to Objects

Once you have given the user access to the servers, the next step is to enter the level of authority the user has to objects on the System i5 if you plan on setting any of the servers to Level 4.

1. If you used F9 from the previous screen, skip to Step 4.

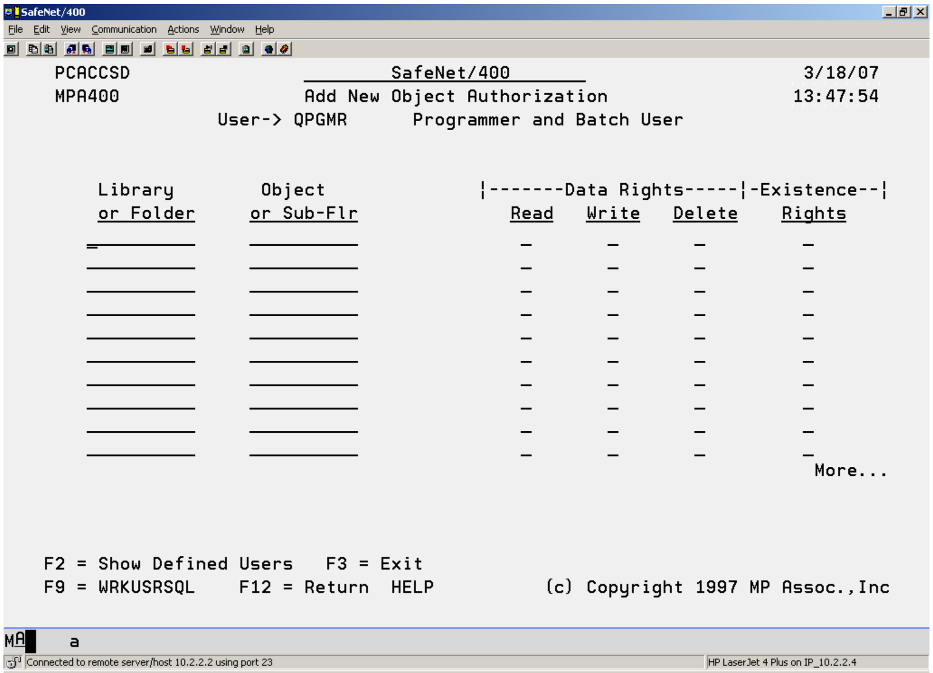
2. If you are currently on the <u>SafeNet/400 Main Menu</u>, select **Option 3 - Work with User to Object Level Security** or use **WRKUSROBJ** command

   The *Work User to Object Security* screen is displayed.

3. Type **the user profile name, the Group** or ***PUBLIC**, then **ENTER.**

   To list all of the user profiles on the system, press **F4** or type ***ALL.**

   To see a list of users already defined within **SafeNet/400** type ***ALLDFN**.



```
    PCACCSD                     SafeNet/400                         3/18/07
    MPA400                Add New Object Authorization             13:47:54
                   User-> QPGMR      Programmer and Batch User


        Library        Object             |-------Data Rights-----|-Existence--|
        or Folder      or Sub-Flr            Read    Write   Delete    Rights
       __________     __________              _       _       _          _
       __________     __________              _       _       _          _
       __________     __________              _       _       _          _
       __________     __________              _       _       _          _
       __________     __________              _       _       _          _
       __________     __________              _       _       _          _
       __________     __________              _       _       _          _
       __________     __________              _       _       _          _
       __________     __________              _       _       _          _
       __________     __________              _       _       _          _
                                                                          More...



   F2 = Show Defined Users    F3 = Exit
   F9 = WRKUSRSQL     F12 = Return  HELP          (c) Copyright 1997 MP Assoc.,Inc

MA     a
```

Connected to remote server/host 10.2.2.2 using port 23   HP LaserJet 4 Plus on IP_10.2.2.4

The *Add New Object Authorization* screen appears.

If you would like to see the list of all users who have been defined within **SafeNet/400**, press **F2.**

Note: If this user has already been set up in **SafeNet/400,** the *Maintain Authorized Objects by User* screen is displayed. **Press F6** to add new objects and authorities for this user.

4. In the *Library or Folder* column, **enter the name** of the library or folder, then **TAB** to the *Object or Sub-Flr* column and **type in the name** of the object or sub-folder.

Note: Allowed entries for **Library** or **Folder**

- *ALLLIB
- *ALLFLR
- Specific library name

When setting up a **library**, you must enter the **complete library name**. Generic library names are not allowed.

Allowed entries for **Object**

- *ALL
- Specific object
- Generic data/program or System i5 object name followed by * (FIL*)

NOT ALLOWED for object

- Long file or folder names - 10 position maximum (names over 10 are truncated)
- Generic sub-folder names (FOLD*)
- Generic folder content names

NOT ALLOWED for library

- Long folder names
- Generic folder names
- Generic library names
- *ALL

If granting rights to multiple objects in one library, you must list the library name multiple times or use a generic object name. For example:

LIBRARY	OBJECT
QUSRSYS	PAY1
QUSRSYS	PROJECT
QUSRSYS	PRT*

5. For *Data Rights*, **type an X** under the appropriate level of authority. Place an X for each data right that applies.

6. For *Existence Rights*, **type an X** if this user will be able to create, delete or move an object.

   To assign EXCLUSIONS to objects and/or libraries, give the user no rights by leaving the *Data Rights* and *Existence Rights* columns blank.

7. Repeat these steps for each object or group of objects for this user profile.

   PageDown to the next screen if you need more lines.

   ENTER when you have finished keying in all necessary objects and rights.

   The *Maintain Authorized Objects by User* screen is refreshed and all the information you just entered is displayed.

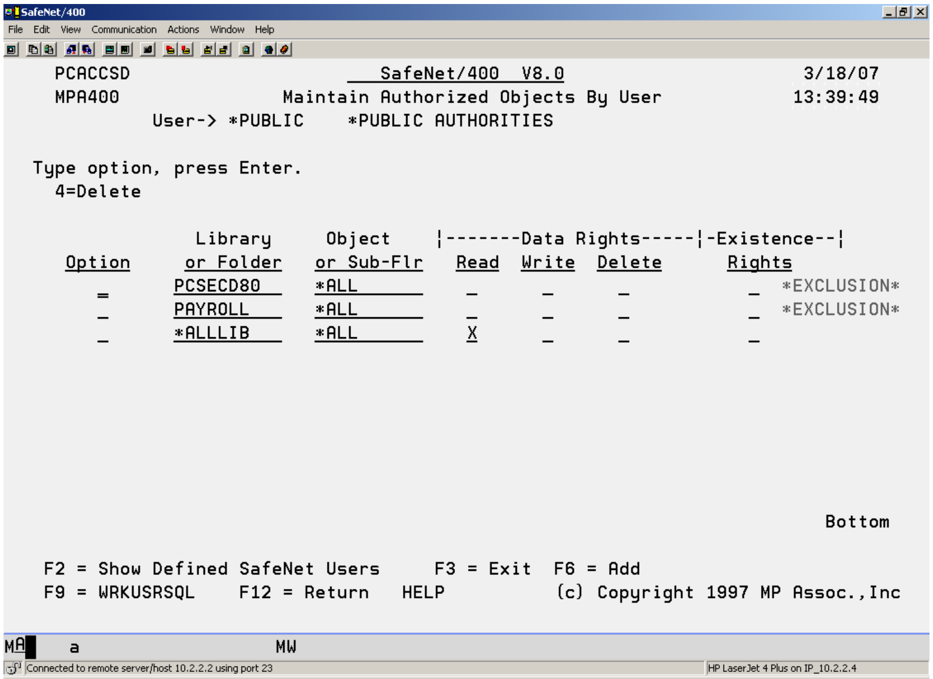
   Press F9 to continue to the next step - setting up user authorities to SQL statements.

   Reminder:

   If you have already entered objects for a particular user, and you are updating their user to object level security, a list of existing object authorities will be displayed. To add more, **press F6**. To delete an existing entry, **type 4** in the *Option* column, then **ENTER.**

Exclusions

To give all users read access to all objects in all libraries, but exclude them from any objects in the PAYROLL library, give *PUBLIC READ authority to the library and exclude *PUBLIC from the PAYROLL library.

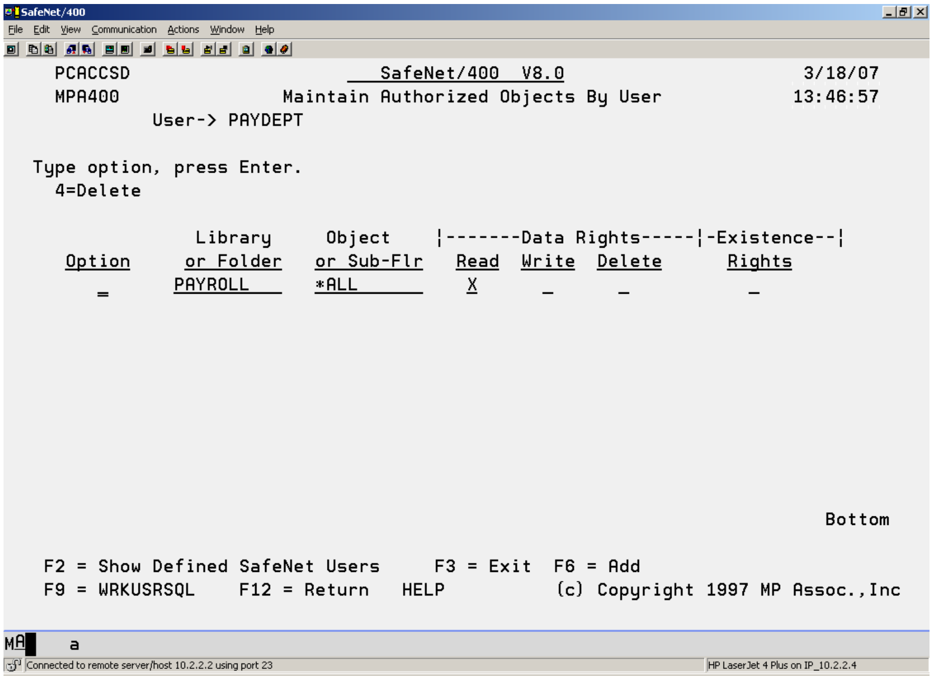


```
     PCACCSD                           SafeNet/400  V8.0                      3/18/07
     MPA400               Maintain Authorized Objects By User            13:39:49
              User-> *PUBLIC    *PUBLIC AUTHORITIES

   Type option, press Enter.
     4=Delete

                  Library     Object    |-------Data Rights-----|-Existence--|
      Option     or Folder   or Sub-Flr   Read  Write  Delete      Rights
         =      PCSECD80     *ALL          _      _      _           _  *EXCLUSION*
         _      PAYROLL      *ALL          _      _      _           _  *EXCLUSION*
         _      *ALLLIB      *ALL          X      _      _           _








                                                                            Bottom

    F2 = Show Defined SafeNet Users     F3 = Exit  F6 = Add
    F9 = WRKUSRSQL    F12 = Return   HELP          (c) Copyright 1997 MP Assoc.,Inc

MA    a                  MW
```

Connected to remote server/host 10.2.2.2 using port 23

HP LaserJet 4 Plus on IP_10.2.2.4

If the PAYDEPT profile needs to use objects in the PAYROLL library, grant user profile PAYDEPT READ authority to the PAYROLL library.


SafeNet/400
File Edit View Communication Actions Window Help

```
  PCACCSD                     SafeNet/400  V8.0                    3/18/07
  MPA400              Maintain Authorized Objects By User          13:46:57
           User-> PAYDEPT

Type option, press Enter.
  4=Delete

              Library     Object    ¦-------Data Rights-----¦-Existence--¦
   Option    or Folder  or Sub-Flr   Read  Write  Delete      Rights
     _      PAYROLL     *ALL          X      _      _           _




                                                                   Bottom

 F2 = Show Defined SafeNet Users     F3 = Exit  F6 = Add
 F9 = WRKUSRSQL    F12 = Return   HELP          (c) Copyright 1997 MP Assoc.,Inc
```

MA   a
Connected to remote server/host 10.2.2.2 using port 23
HP LaserJet 4 Plus on IP_10.2.2.4

This individual authority overrides the *PUBLIC authority.

Entering User Authorities to SQL Statements

If you are going to set the *SQL* servers to Level 4 only, the next step is to authorize users to the SQL Statements they may need.

1. If you used F9 from the previous screen, skip to Step 4.

2. If you are currently on the <u>SafeNet/400 Main Menu</u>, select **Option 4 - Work with User to SQL Statement Security** or use **WRKUSRSQL** command

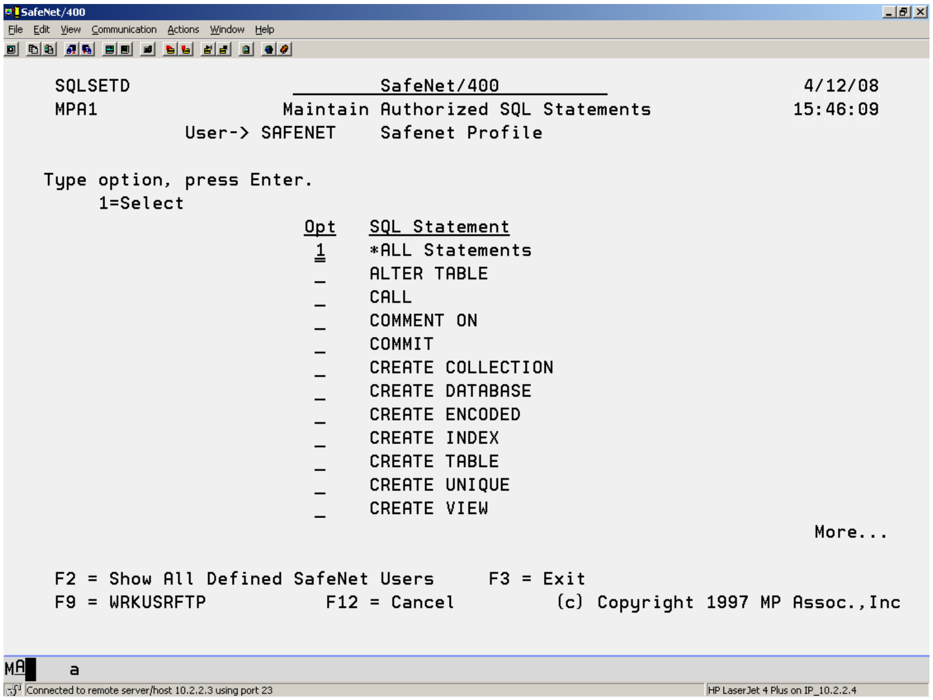
   The *Work User to SQL Statements* screen is displayed.

3. **Type the user profile, the Group** or ***PUBLIC**, then **ENTER**.

   If you would like a list of all user profiles on the system, press **F4** or type ***ALL**.

   To see a list of users already defined within **SafeNet/400** type ***ALLDFN**.

   The *Maintain Authorized SQL Statements* screen appears.



```
    SQLSETD                  SafeNet/400                         4/12/08
    MPA1               Maintain Authorized SQL Statements        15:46:09
                User-> SAFENET    Safenet Profile

   Type option, press Enter.
        1=Select
                             Opt   SQL Statement
                              1    *ALL Statements
                              _    ALTER TABLE
                              _    CALL
                              _    COMMENT ON
                              _    COMMIT
                              _    CREATE COLLECTION
                              _    CREATE DATABASE
                              _    CREATE ENCODED
                              _    CREATE INDEX
                              _    CREATE TABLE
                              _    CREATE UNIQUE
                              _    CREATE VIEW
                                                                      More...

    F2 = Show All Defined SafeNet Users     F3 = Exit
    F9 = WRKUSRFTP           F12 = Cancel         (c) Copyright 1997 MP Assoc.,Inc

MA     a
Connected to remote server/host 10.2.2.3 using port 23                HP LaserJet 4 Plus on IP_10.2.2.4
```

4. **Type 1** in front of each SQL statement that this user is permitted to use.

   Selecting ***ALL Statements** authorizes the use to all SQL statements

   To remove authorization to a selection, remove the 1.

If you would like to see the list of all users who have been defined within **SafeNet/400**, press **F2.**

5. When finished making all your selections, **ENTER**.

6. **Press F9** to advance to the next step - setting up user authorities to FTP statements.

Entering User Authorities to FTP Statements

Next you must authorize users to the FTP Statements they may need if you are going to set the *FTP Server* or *FTP Client* to Level 4.

1. If you used F9 from the previous screen, continue with Step 4.

2. If you are on the SafeNet/400 Main Menu, select **Option 5 - Work with User to FTP Statement Security** or use **WRKUSRFTP** command

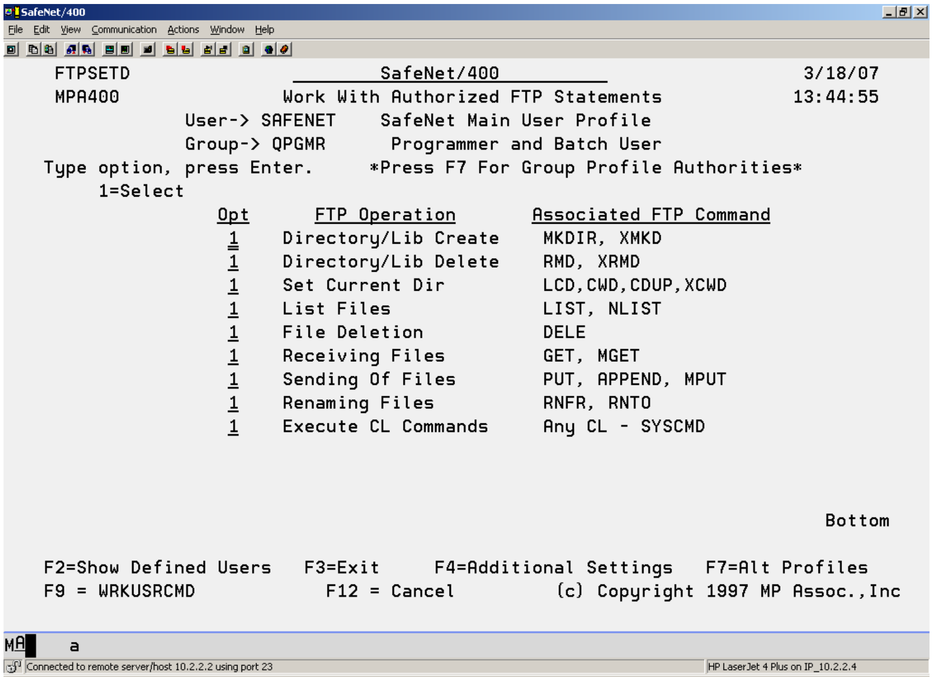
   The *Work User to FTP Statements, Enter User ID* screen is displayed.

3. **Type the user profile** or ***PUBLIC** then **ENTER**.

   If you would like a list of all user profiles on the system, press **F4** or type ***ALL**.

   To see a list of users already defined within **SafeNet/400** type ***ALLDFN**.

   The *Work with Authorized FTP Statements* screen appears.



```
    FTPSETD                   SafeNet/400                        3/18/07
    MPA400               Work With Authorized FTP Statements      13:44:55
                User-> SAFENET    SafeNet Main User Profile
                Group-> QPGMR      Programmer and Batch User
   Type option, press Enter.     *Press F7 For Group Profile Authorities*
        1=Select
                   Opt      FTP Operation        Associated FTP Command
                    1    Directory/Lib Create     MKDIR, XMKD
                    1    Directory/Lib Delete     RMD, XRMD
                    1    Set Current Dir          LCD,CWD,CDUP,XCWD
                    1    List Files               LIST, NLIST
                    1    File Deletion            DELE
                    1    Receiving Files          GET, MGET
                    1    Sending Of Files         PUT, APPEND, MPUT
                    1    Renaming Files           RNFR, RNTO
                    1    Execute CL Commands      Any CL - SYSCMD



                                                                      Bottom

   F2=Show Defined Users   F3=Exit     F4=Additional Settings   F7=Alt Profiles
   F9 = WRKUSRCMD            F12 = Cancel         (c) Copyright 1997 MP Assoc.,Inc

MA     a
```

Connected to remote server/host 10.2.2.2 using port 23
HP LaserJet 4 Plus on IP_10.2.2.4

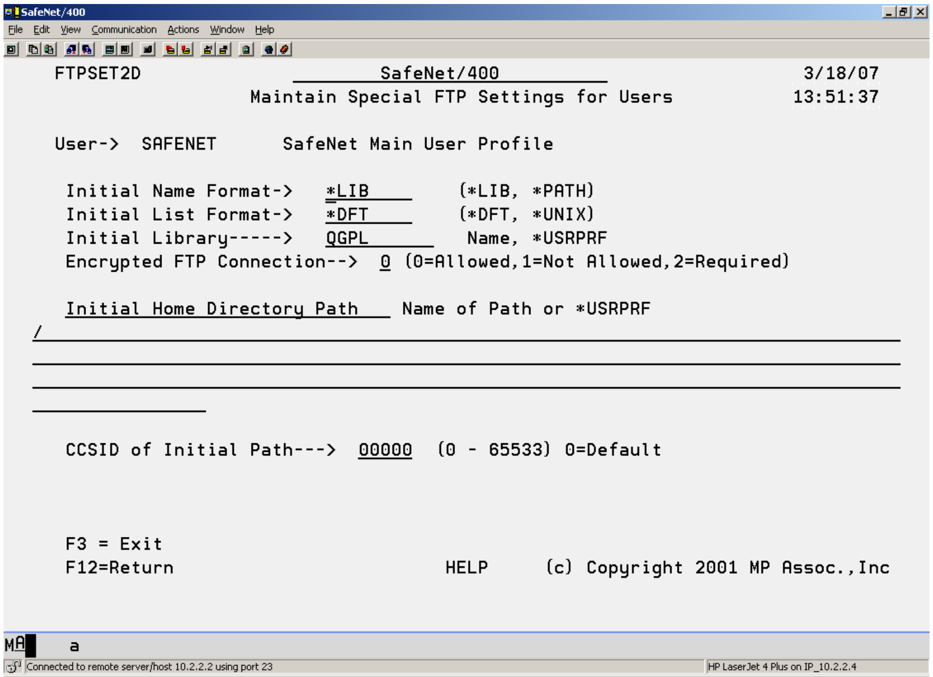
4. **Type 1** in front of each FTP statement that this user is permitted to use.

   To remove authorization to a statement, remove the 1.

If you would like to see the list of all users who have been defined within **SafeNet/400**, press **F2**.

5. Press F4 to display the *Maintain Special FTP Settings for Users* screen

Note: Special FTP settings for a user are allowed only when your system is at OS/400 V5R1 or higher. If you are at a previous operating system level, these settings have no effect.



```
   FTPSET2D                   SafeNet/400                              3/18/07
                      Maintain Special FTP Settings for Users         13:51:37

   User->  SAFENET      SafeNet Main User Profile

    Initial Name Format->   *LIB         (*LIB, *PATH)
    Initial List Format->   *DFT         (*DFT, *UNIX)
    Initial Library----->   QGPL          Name, *USRPRF
    Encrypted FTP Connection-->  0 (0=Allowed,1=Not Allowed,2=Required)

    Initial Home Directory Path     Name of Path or *USRPRF
 /

    CCSID of Initial Path--->   00000  (0 - 65533) 0=Default

    F3 = Exit
    F12=Return                          HELP     (c) Copyright 2001 MP Assoc.,Inc

MA     a
Connected to remote server/host 10.2.2.2 using port 23        HP LaserJet 4 Plus on IP_10.2.2.4
```

For this user, the initial Name Format and List Format will override the settings established by the OS/400 Change FTP Server Attributes command (CHGFTPA).

Select the parameters as follows:

Encrypted

- For SSL connections this should be set to 0 or 2
- For regular or non-SSL connections, leave this set to 0 or 1

PATH

This field is in effect only when Name Format is set to *UNIX. The field should point to an actual IFS directory on the System i5.

Name Format

- *LIB indicates that the user sees standard Library/Object OS/400 style names
- *PATH displays PC or *UNIX style file and directory names.

List Format

- *DFT user sees standard OS/400 CHGFTPA server settings
- *UNIX user sees UNIX style directory listings

6. When finished making all your selections, **ENTER**.

7. **Press F9** to continue to the next step - setting up user authorities to CL commands.

Important Note:

When the FTP Client point is set to Level 4, only the GET and PUT FTP sub-commands are required. The other commands, when using the FTP Client, are for the TARGET SYSTEM ONLY (sent to/run on the target system).

When authorizing users to the GET/PUT sub-commands, the assumed object authority is reversed from authorities required for the FTP Server point and the same objects.

See the following examples.

Using FTP Client:

- Sending an object to a remote system
  An FTP PUT of object ABC in an FTP Client session requires *READ authority to object ABC on the local machine.
- Get an object from a remote system
  An FTP GET of object ABC in an FTP Client session requires *OBJMGT authority to the object ABC on the local machine.

Using FTP Server:

- Send an object to local system
  An FTP PUT of object ABC in an FTP Server session requires *OBJMGT authority to the object ABC on the LOCAL machine.
- Get an object from the local system
  An FTP GET of object ABC in an FTP Server session requires *READ authority to the object ABC on the LOCAL machine.

Next, if you plan on setting the *FTP*, *DDM* or *Remote Command Servers* to Level 4, you must authorize users to the CL commands they may need.

1. If you used F9 from the previous screen, continue with Step 4.

2. From the SafeNet/400 Main Menu, select **Option 6 - Work with User to CL Command Security** or use **WRKUSRCMD** command

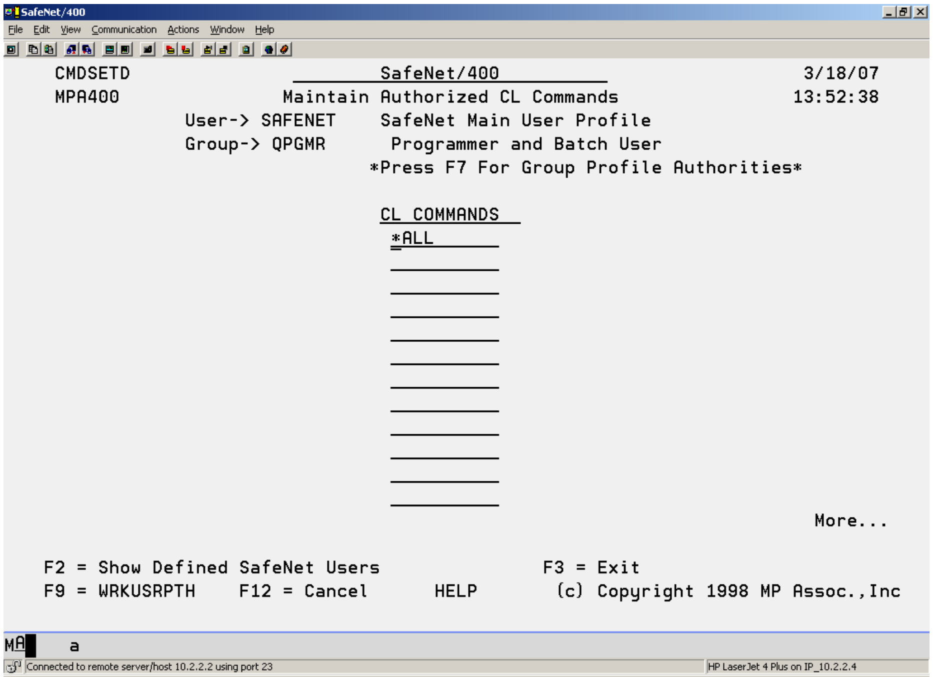
   The *Work User to CL Commands, Enter User ID* screen is displayed.

3. **Type the user profile** or ***PUBLIC** then **ENTER**.

   If you would like a list of all user profiles on the system, press **F4** or type ***ALL**.

   To see a list of users already defined within **SafeNet/400** type ***ALLDFN**.

   The *Maintain Authorized CL Commands* screen appears.



```
   CMDSETD                       SafeNet/400                          3/18/07
   MPA400              Maintain Authorized CL Commands                13:52:38
               User-> SAFENET    SafeNet Main User Profile
               Group-> QPGMR      Programmer and Batch User
                                *Press F7 For Group Profile Authorities*

                                 CL COMMANDS
                                  *ALL____
                                  __________
                                  __________
                                  __________
                                  __________
                                  __________
                                  __________
                                  __________
                                  __________
                                  __________
                                  __________
                                  __________
                                                                       More...

  F2 = Show Defined SafeNet Users              F3 = Exit
  F9 = WRKUSRPTH    F12 = Cancel      HELP      (c) Copyright 1998 MP Assoc.,Inc

MA     a
Connected to remote server/host 10.2.2.2 using port 23          HP LaserJet 4 Plus on IP_10.2.2.4
```

4. **Type each CL command that this user is permitted to use.**

   If you want the user to have access to all CL commands, **type *ALL** in the first available space.

To remove authorization to a command, **FIELD EXIT** through the line to blank it out.

If you would like to see the list of all users who have been defined within **SafeNet/400**, press **F2**.

5. When finished typing all the required CL commands for this user, press **ENTER**.

6. **Press F9** to continue with setting up path names.

Entering Long Path Names

The default **SafeNet/400** setting is to use long path names.

If you choose to not use long path name support, you must first change the **SafeNet/400** default setting. Use the **CHGSPCSET** command to set the *PATHL* parameter to **SHORT*.

Follow these steps to authorize the user to the paths.

1. If you used F9 from the previous screen, continue with Step 4.

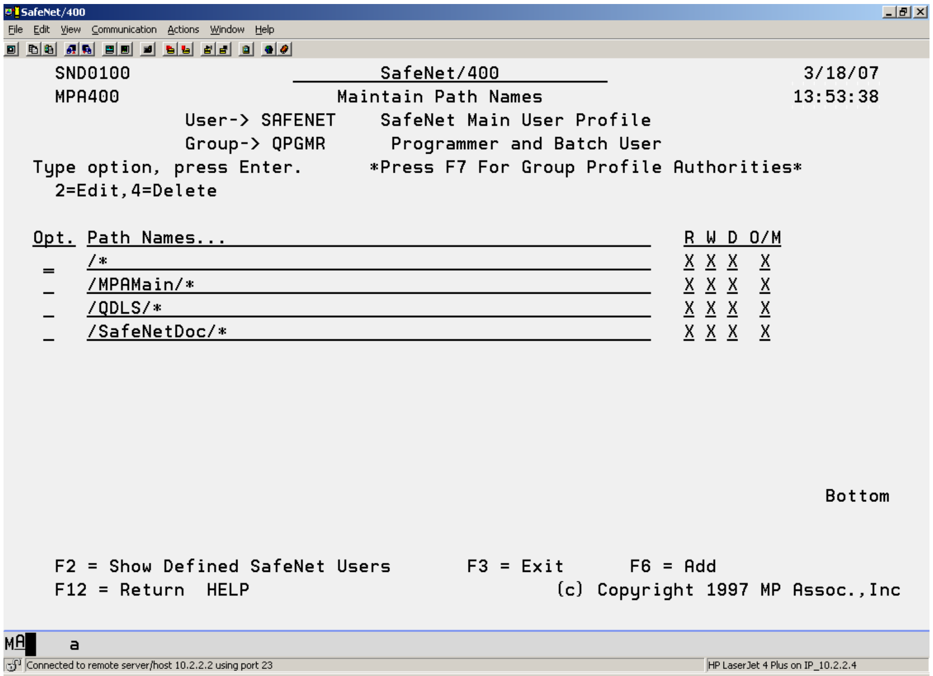
2. From the SafeNet/400 Main Menu, select **Option 7 - Work with User to Long Path Names** or use **WRKUSRPTH** command

   The *Work with User to Path Names, Enter User ID* screen is displayed.

3. **Type the user profile or *PUBLIC** then **ENTER**.

   If you would like a list of all user profiles on the system, press **F4** or type ***ALL**.

   To see a list of users already defined within **SafeNet/400** type ***ALLDFN**.



```
    SND0100                    SafeNet/400                         3/18/07
    MPA400                  Maintain Path Names                   13:53:38
                User-> SAFENET    SafeNet Main User Profile
                Group-> QPGMR      Programmer and Batch User
  Type option, press Enter.      *Press F7 For Group Profile Authorities*
    2=Edit,4=Delete

  Opt. Path Names...                                      R W D O/M
   _   /*                                                 X X X  X
   _   /MPAMain/*                                         X X X  X
   _   /QDLS/*                                            X X X  X
   _   /SafeNetDoc/*                                      X X X  X

                                                                      Bottom

    F2 = Show Defined SafeNet Users       F3 = Exit      F6 = Add
    F12 = Return  HELP                           (c) Copyright 1997 MP Assoc.,Inc

MA     a
Connected to remote server/host 10.2.2.2 using port 23          HP LaserJet 4 Plus on IP_10.2.2.4
```

The *Maintain Path Names* screen appears.

If you would like to see the list of all users who have been defined within **SafeNet/400**, press **F2**.

4. Enter the paths that the user is authorized to.

   Paths can be entered up to 256 positions in length, although only the first 60 positions are shown on the display. To enter and/or view a path over 60 positions long, **enter 2** in the option column.

   Use /* to give authority to all folders/paths

   End the path with * to allow access to all items in subfolders.

5. When finished typing all the paths for this user, press **ENTER**.

Copying an Existing User to Set Up a New User in SafeNet/400

This will allow you to copy the authorities and settings from one user to another within **SafeNet/400**. The new user profile must already exist in OS/400.

1. From the Special Jobs Menu, select **Option 13 – Copy a User Setup to Another User** or use the **CPYSNUSR** command.

   The *Copy SafeNet User/Authorities* screen is displayed.

2. **Type the user profile** you are copying from, then **the new profile(s)** to add.

3. When finished entering all the new profiles, press **ENTER**.

   This will set up the new profile in **SafeNet/400** and return you to the Special Jobs Menu.

Removing a User from SafeNet/400

This option allows you to remove a user's authorities and settings from **SafeNet/400.**

1. From the Special Jobs Menu select **Option 14 – Remove a User Enrollment from SafeNet** or use the **RMVSNUSR** command

   The *Remove Users from SafeNet* screen appears.

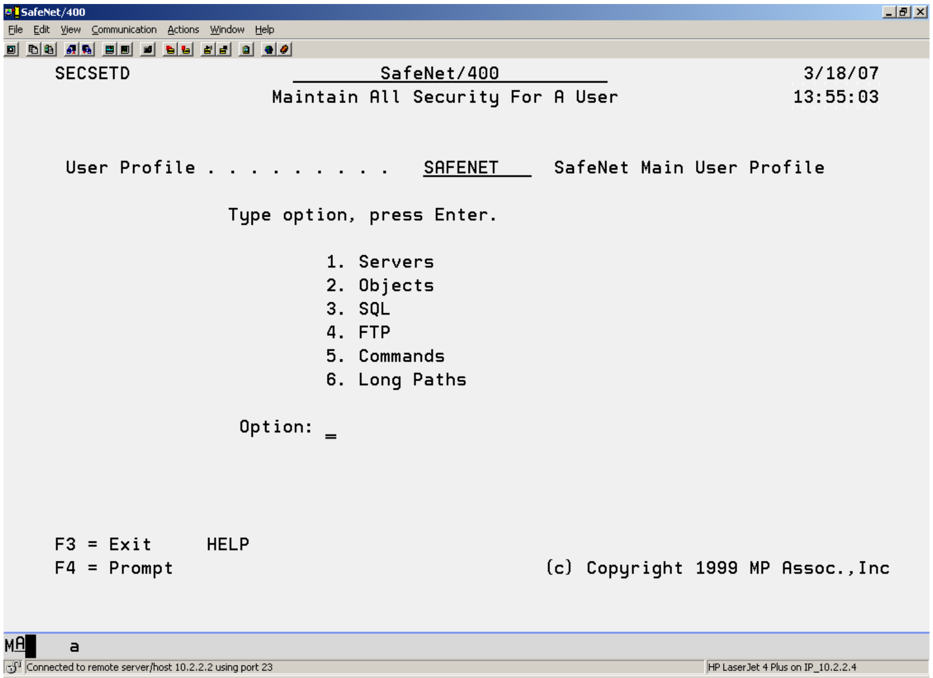
2. **Type the user profile(s)** to remove, then press ENTER.

   This will remove the user from **SafeNet/400** and return you to the Special Jobs Menu.

Maintain all Security for a User

The **WRKUSRSEC** command, which is not found on any of the **SafeNet/400** menus, gives you the ability to perform security maintenance for an individual user without entering several different commands.

When you use the **WRKUSRSEC** command you will be presented with the *Maintain All Security for a User* screen.



```
   SECSETD                   SafeNet/400                        3/18/07
                      Maintain All Security For A User          13:55:03


    User Profile . . . . . . . . .   SAFENET     SafeNet Main User Profile

                    Type option, press Enter.

                            1. Servers
                            2. Objects
                            3. SQL
                            4. FTP
                            5. Commands
                            6. Long Paths

                     Option: _



   F3 = Exit     HELP
   F4 = Prompt                             (c) Copyright 1999 MP Assoc.,Inc

MA      a
Connected to remote server/host 10.2.2.2 using port 23        HP LaserJet 4 Plus on IP_10.2.2.4
```

From this screen you can select which of the control files you wish to update for this particular user, without entering any additional commands or returning to the SafeNet/400 Main Menu.

Within each of the applications, you can use **F9** to advance to the next maintenance screen.

Setting up Time of Day Controls

If you want to exclude users from server functions based on the day of the week or the time of day, use Time of Day controls.

SafeNet/400 checks authority in the following sequence:

Is the	**authorized to**	**at this time?**
User	Specific Server *ALL Servers	
Group	Specific Server *ALL Servers	
Supplemental Group	Specific Server *ALL Servers	
*PUBLIC	*Specific Server *ALL Servers	

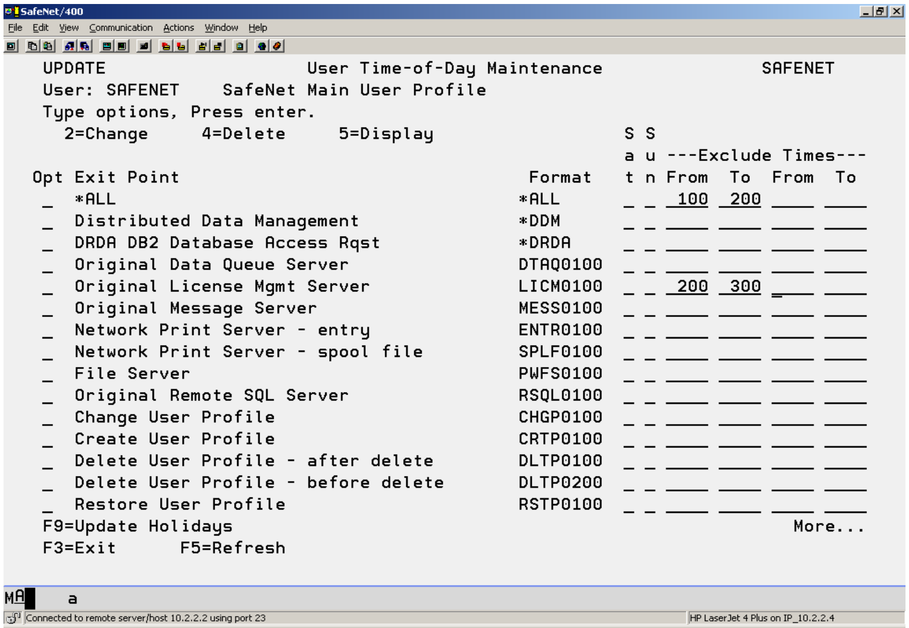
SafeNet/400 checks until all the tests are passed or until an exclusion rule is encountered.

Note: In Version 8, Time of Day controls are handled differently than in previous releases of SafeNet/400. With Version 8, TOD controls are activated at the server level. Use the WRKSRV command to turn on Time of Day checking on the appropriate servers.

To set up the Time of Day controls for a specific user, use **Option 2 – Work with User to Server Security** from the <u>SafeNet/400 Main Menu</u> or the **WRKUSRSRV** command.

Type the user profile, **ENTER** and then **press F10**.

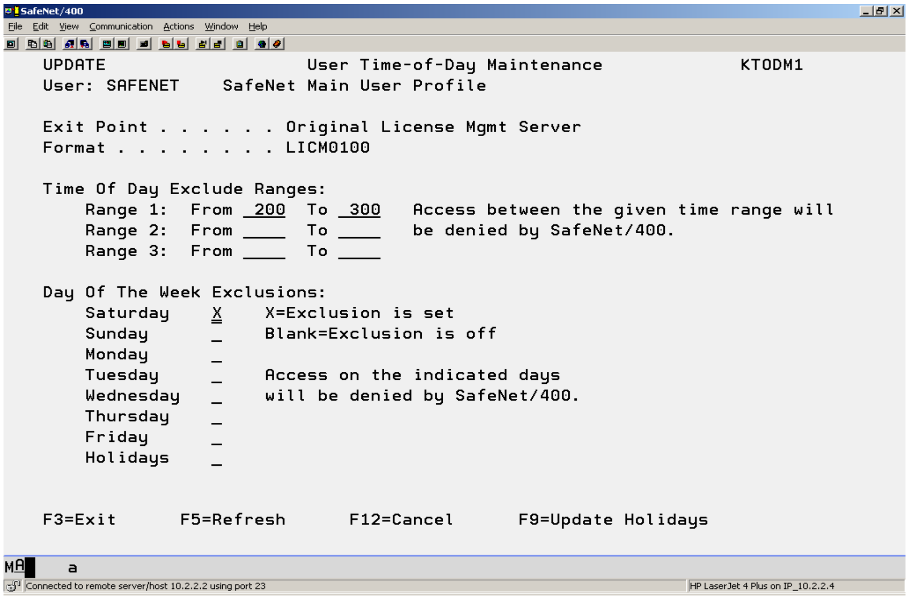
The *User Time-of-Day Maintenance* screen appears.


SafeNet/400
File Edit View Communication Actions Window Help
MA a
Connected to remote server/host 10.2.2.2 using port 23
HP LaserJet 4 Plus on IP_10.2.2.4

```
 UPDATE                   User Time-of-Day Maintenance              SAFENET
 User: SAFENET    SafeNet Main User Profile
 Type options, Press enter.
   2=Change     4=Delete     5=Display                 S S
                                                       a u ---Exclude Times---
Opt Exit Point                                Format   t n From  To  From  To
 _  *ALL                                      *ALL     _ _  100  200 ____ ____
 _  Distributed Data Management               *DDM     _ _ ____ ____ ____ ____
 _  DRDA DB2 Database Access Rqst             *DRDA    _ _ ____ ____ ____ ____
 _  Original Data Queue Server                DTAQ0100 _ _ ____ ____ ____ ____
 _  Original License Mgmt Server              LICM0100 _ _  200  300 ____ ____
 _  Original Message Server                   MESS0100 _ _ ____ ____ ____ ____
 _  Network Print Server - entry              ENTR0100 _ _ ____ ____ ____ ____
 _  Network Print Server - spool file         SPLF0100 _ _ ____ ____ ____ ____
 _  File Server                               PWFS0100 _ _ ____ ____ ____ ____
 _  Original Remote SQL Server                RSQL0100 _ _ ____ ____ ____ ____
 _  Change User Profile                       CHGP0100 _ _ ____ ____ ____ ____
 _  Create User Profile                       CRTP0100 _ _ ____ ____ ____ ____
 _  Delete User Profile - after delete        DLTP0100 _ _ ____ ____ ____ ____
 _  Delete User Profile - before delete       DLTP0200 _ _ ____ ____ ____ ____
 _  Restore User Profile                      RSTP0100 _ _ ____ ____ ____ ____
 F9=Update Holidays                                                    More...
 F3=Exit      F5=Refresh
```

To exclude the user from all servers during the same days of the week and time of day, **type 2 –** *Change* in front of *ALL.

To select individual servers, type 2 in front of the servers you want to change

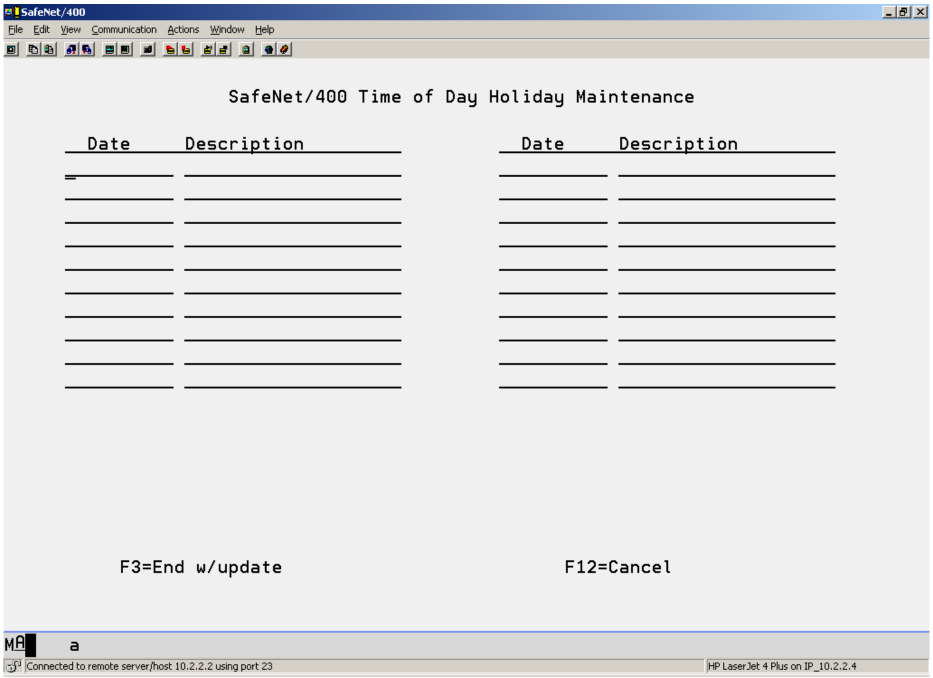

SafeNet/400
File Edit View Communication Actions Window Help
MA a
Connected to remote server/host 10.2.2.2 using port 23
HP LaserJet 4 Plus on IP_10.2.2.4

```
 UPDATE                   User Time-of-Day Maintenance            KTODM1
 User: SAFENET    SafeNet Main User Profile

 Exit Point . . . . . . Original License Mgmt Server
 Format . . . . . . . . LICM0100

 Time Of Day Exclude Ranges:
     Range 1:  From  200  To  300   Access between the given time range will
     Range 2:  From ____  To ____   be denied by SafeNet/400.
     Range 3:  From ____  To ____

 Day Of The Week Exclusions:
     Saturday    X    X=Exclusion is set
     Sunday      _    Blank=Exclusion is off
     Monday      _
     Tuesday     _    Access on the indicated days
     Wednesday   _    will be denied by SafeNet/400.
     Thursday    _
     Friday      _
     Holidays    _


 F3=Exit      F5=Refresh      F12=Cancel      F9=Update Holidays
```

You can define up to three time ranges and can select which days to exclude by typing **X** in front of the day.

You can also define holidays that will be used to control Time of Day access.

Press F9 to display the Time of Day Holiday Maintenance screen.


SafeNet/400
File Edit View Communication Actions Window Help

```
                 SafeNet/400 Time of Day Holiday Maintenance

      Date      Description                        Date      Description
    __________  ____________________           __________  ____________________
    __________  ____________________           __________  ____________________
    __________  ____________________           __________  ____________________
    __________  ____________________           __________  ____________________
    __________  ____________________           __________  ____________________
    __________  ____________________           __________  ____________________
    __________  ____________________           __________  ____________________
    __________  ____________________           __________  ____________________
    __________  ____________________           __________  ____________________
    __________  ____________________           __________  ____________________



         F3=End w/update                          F12=Cancel
```

MA a
Connected to remote server/host 10.2.2.2 using port 23
HP LaserJet 4 Plus on IP_10.2.2.4

Type the dates and descriptions of your holidays.

Press **ENTER**.

Chapter 2 - SETTING UP SERVERS

The final step in configuring **SafeNet/400** is to enter the Security Level settings for all the server functions.

Important:	If you do this step first and restrict access to the server functions prior to setting up user rights, you may disrupt network requests until the users' authority table setup is completed. Setting up the Current Level on the servers should be considered the **LAST STEP** during the setup process.

Typically use the Future Server Settings for initial setup and testing. When you are ready to activate SafeNet/400 settings, flip the current and future settings using the WRKSRV command, F22.

SafeNet/400 Server Function Security Levels

Level 1:

- IBM default
- Unlimited access, all requests accepted
- Requests can be logged, reporting available
- Performance impact - none

Level 2:

- No access at all, all requests for server are rejected
- Requests can be logged, reporting available
- Performance impact - not a consideration

Level 3:

- Access granted on a user-by-user basis to the server
- Requests can be logged, reporting available
- Performance impact – minimal
- TELNET requires use of the TCP/IP control table

Level 4:

- Access granted on a user to server and object and command basis
- Requests can be logged, reporting available
- Performance impact – higher

Level 4 requires authority to the server function and additionally requires table entries for proper authorization to individual or generic objects and/or folders by user profile. Data rights such as read/write and object management rights can be assigned on an individual basis.

Level 4 on the *DDM, FTP* or *Remote Command/Program Call Server* requires setting up authorities to CL commands.

For *DDM, FTP* or *Remote Command/Program Call Server,* all commands are restricted.

Level 5:

- This indicates that **SafeNet/400** does not recognize a program assigned to the exit point or has detected a user-defined program assigned. (Use WRKREGINF command to review existing exit point programs.)
- Not supported
- Cannot be changed via **SafeNet/400**, use WRKREGINF command
- See Appendix A, 'Special Technical Considerations'

On the following pages you will find these levels grouped together to make it easier for you to decide the appropriate level of security required for each server function.

Setting the Server Function Logging Levels

The valid logging levels are:

Logging Level A	Log all transactions
Logging Level R	Log only rejected requests
Logging Level N	No logging

As you set up your Server Function logging levels, please remember the following:

- If you set the logging level on the Server Function to *NO LOGGING* or *REJECTIONS*, the Server Function setting will override the individual user logging level.

- If you set the logging level on the Server Function to *ALL*, the individual user logging level will override the Server Function logging level.

To make sure you are logging transactions correctly, we recommend that when you initially set up **SafeNet/400** you set the Server Functions to log *ALL* and set the individual user logging levels to either *ALL* or *REJECTIONS*.

Then, after you have had some experience with checking the logs and interpreting the results, you may want to make changes for specific user and server combinations.

Basic Server Security - Supported by all Servers

Level 1 - IBM Default

Level 2 - No access to server

Intermediate Server Security - Supported by all Servers

Level 3 - Users must be authorized to the server

Special
Level 3 - *TELNET - controls signon by IP address

Advanced Server Security - Supported by Specific Servers

Level 4 - The user must be authorized to the server, the objects requested, the FTP Op or SQL Op, CL commands or long path to be used.

Supported by the following servers:

- Distributed Data Management Server
- Original Data Queue Server
- Network Printer Server - Spool file requests
- Integrated File Server
- Original Remote SQL Server
- Original File Transfer Function Server
- Original Virtual Print Server
- Database Server - Data base access
- Database Server - SQL access
- Data Queue Server
- Remote Command/Program Call Server
- FTP Server Request Validation
- FTP Client Request Validation
- REXEC Server request Validation
- Showcase Strategy** Server

Recommended Server Settings

Server Description	Recommended Setting
Central Server - client management	**Level 1, Log None**
Central Server - conversion map	**Level 1, Log None**
Central Server - license management	**Level 1, Log None**
Database Server - entry	**Level 3, Log All**- Limit user access
Database Server - data base access - 100	**Level 4, Log All** - Limit user and object access
Database Server - data base access - 200	**Level 4, Log All** - Limit user and object access
Database Server - object information - 100	**Level 3, Log All** - Limit user access
Database Server - object information - 200	**Level 3, Log All** - Limit user access
Database Server - SQL access - 100	**Level 4, Log All** - Limit user, object and SQL statement access
Database Server - SQL access – 200	**Level 4, Log All -** Limit user, object and SQL statement access
Data Queue Server	**Level 1, Log None**

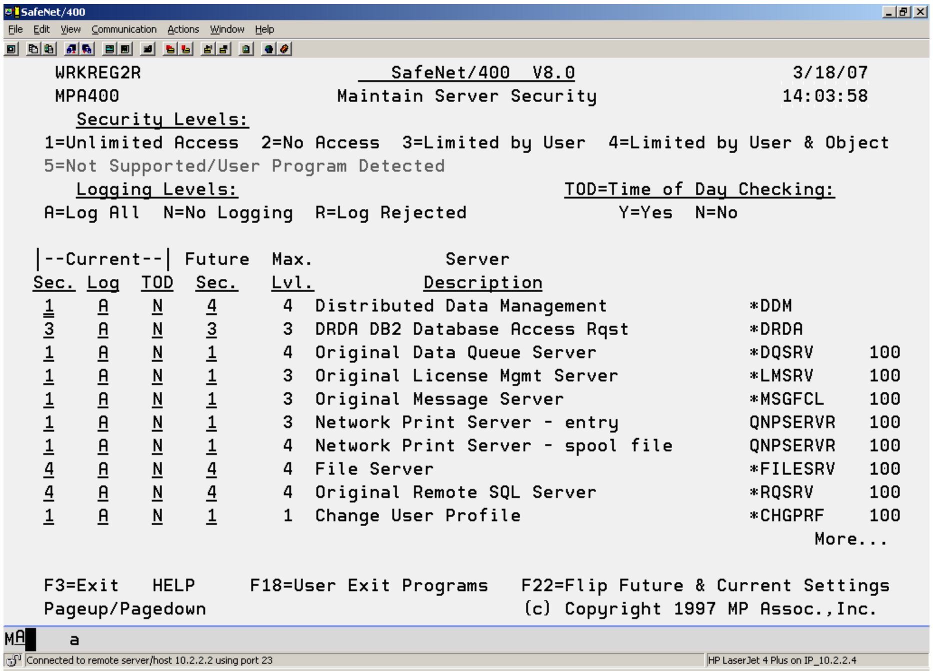
Server Description	Recommended Setting
Distributed Data Management	**Level 3, Log All -** Limit user access or **Level 4, Log All** - Limit users to specific objects and commands
DHCP	**Level 1, Log None**
DRDA DB2 Database Access Request	**Level 3, Log All -** Limit user
File Server	**Level 4, Log All** - Limit user and object access
FTP Client Server	**Level 4, Log All** - Limit user access & target connection by IP Address
FTP Logon Server	**Level 3, Log All** - Limit user access
FTP Server Validation	**Level 4, Log All** - Limit user, source IP address, object, FTP sub-commands
Network Print Server - entry	**Level 1, Log None**
Network Print Server - spool file	**Level 1, Log None**
Original Data Queue Server	**Level 1, Log None**
Original File Transfer Function	**Level 4, Log All** - Limit user and object access
Original License Mgmt Server	**Level 1, Log None**

Server Description	Recommended Setting
Original Message Server	**Level 1, Log None**
Original Remote SQL Server	**Level 4, Log All -** Limit user access to objects and SQL statements
Original Virtual Print Server	**Level 1, Log None**
PWRDWNSYS	**Level 1, Log All –** Log all requests
Remote Command/Program Call	**Level 4, Log All -** Limit user and object access and commands
REXEC Logon	**Level 3, Log All -** Limit user access
REXEC Server Request Validation	**Level 4, Log All -** Limit user, Source IP address
TELNET Logon **or** **TELNET Logoff**	**Level 1, Log None**
TFTP Logon	**Level 1, Log None**
User Profile Points	**Level 1, Log All -** Log all requests
TCP Signon Server	**Level 1, Log None**
Showcase Strategy Server**	**Level 4, Log All –** Limit User,Object, Log all

Entering Server Function Security Levels

1. From the <u>SafeNet/400 Main Menu</u> select **Option 1 - Work with Server Security Settings** or use **WRKSRV** command

   The *Maintain Server Security* screen is displayed.



```
    WRKREG2R                     SafeNet/400  V8.0                3/18/07
    MPA400                     Maintain Server Security          14:03:58
      Security Levels:
   1=Unlimited Access  2=No Access  3=Limited by User  4=Limited by User & Object
   5=Not Supported/User Program Detected
      Logging Levels:                             TOD=Time of Day Checking:
   A=Log All   N=No Logging  R=Log Rejected               Y=Yes  N=No

  |--Current--| Future  Max.            Server
  Sec. Log  TOD  Sec.   Lvl.          Description
   1    A    N    4      4  Distributed Data Management           *DDM
   3    A    N    3      3  DRDA DB2 Database Access Rqst         *DRDA
   1    A    N    1      4  Original Data Queue Server            *DQSRV     100
   1    A    N    1      3  Original License Mgmt Server          *LMSRV     100
   1    A    N    1      3  Original Message Server               *MSGFCL    100
   1    A    N    1      3  Network Print Server - entry          QNPSERVR   100
   1    A    N    1      4  Network Print Server - spool file     QNPSERVR   100
   4    A    N    4      4  File Server                           *FILESRV   100
   4    A    N    4      4  Original Remote SQL Server            *RQSRV     100
   1    A    N    1      1  Change User Profile                   *CHGPRF    100
                                                                        More...

   F3=Exit   HELP     F18=User Exit Programs    F22=Flip Future & Current Settings
   Pageup/Pagedown                              (c) Copyright 1997 MP Assoc.,Inc.
MA     a
```

Connected to remote server/host 10.2.2.2 using port 23   HP LaserJet 4 Plus on IP_10.2.2.4

2. Enter the level of security and the logging level that is required for each server description in the *Current* columns.

   The *Future* column lets you enter a setting for each server based on what you think the setting will be in the future. This makes it possible to use your historical transactions against both current and future server levels for testing purposes.

   Enter a 'Y" in the TOD column to control individual server functions based on time of day.

   When you change the TOD value it becomes effective immediately. Make sure you have used the *Time of Day* setup function, accessed via F10 within the **WRKUSRSRV** command, before you change this value on the server function.

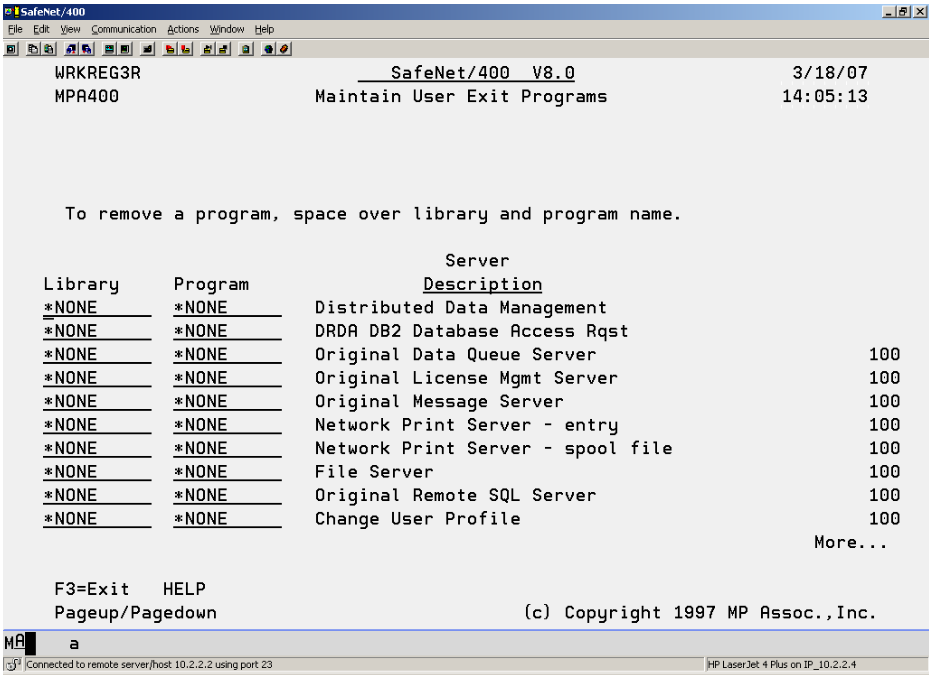
Note: The server functions are listed on multiple screens. **PageDown** to ensure you enter a level for all the servers.

3. When you have finished entering information for all the servers, **press ENTER.**

   The screen is refreshed and any changes you made are reflected in the *Current* columns.

Customer Exit Programs

If you would like to use your own programs over these server exit points, **F18** on the Maintain Server Security screen gives you the ability to do so.


SafeNet/400
File Edit View Communication Actions Window Help
Connected to remote server/host 10.2.2.2 using port 23
HP LaserJet 4 Plus on IP_10.2.2.4

```
     WRKREG3R                       SafeNet/400  V8.0                   3/18/07
     MPA400                  Maintain User Exit Programs               14:05:13



      To remove a program, space over library and program name.

                                          Server
    Library     Program                 Description
    *NONE       *NONE        Distributed Data Management
    *NONE       *NONE        DRDA DB2 Database Access Rqst
    *NONE       *NONE        Original Data Queue Server                       100
    *NONE       *NONE        Original License Mgmt Server                     100
    *NONE       *NONE        Original Message Server                          100
    *NONE       *NONE        Network Print Server - entry                     100
    *NONE       *NONE        Network Print Server - spool file                100
    *NONE       *NONE        File Server                                      100
    *NONE       *NONE        Original Remote SQL Server                       100
    *NONE       *NONE        Change User Profile                              100
                                                                         More...

     F3=Exit   HELP
     Pageup/Pagedown                                (c) Copyright 1997 MP Assoc.,Inc.
MA     a
```

SafeNet/400 will look to see if there is a customer-written program to call. If there is, it calls the program, passing two parameters, a one-byte status code, plus the rest of the data string from the client. The customer exit program is always processed BEFORE the **SafeNet/400** checks are done.

Your custom exit program can do whatever you want. When it returns to **SafeNet/400**, if the status code has been changed to indicate any type of rejection, **SafeNet/400** stops and logs the request, and returns a rejection to the client.

If the exit program does not change the status code, the request will go through the normal **SafeNet/400** checking process.

The string that is passed is limited to 4,000 characters, as defined by IBM. Examples of these strings can be found in the TRAPOD file and the appropriate IBM manuals.

Chapter 3 - TELNET, TCP/IP ADDRESS CONTROLS

Setting up TELNET

TELNET control features are supported only when the server is set to Level 3. You may use some or all of the features available with the TELNET server point:

- Control access by IP address
- Allow auto-signon (bypass signon)
- Restrict IP address to use specific device names (enhanced TELNET clients only)
- Restrict access based on the password type sent (none, clear or encrypted)

Controlling TELNET Access by IP Address

1. Set the TELNET server to Level 3 using the **WRKSRV** command.

2. From the SafeNet/400 Main Menu, select **Option 7 – Work with TCP/IP Address Security** or use the **WRKTCPIPA** command and enter ***TELNET** as the server to control

3. **Enter the IP address** in dotted decimal format (i.e., 10.2.2.2)

   Use wild card options if desired (10.2.2.x)

4. **Enter A or R** to accept or reject the request

Restricting Access to Specific Device Names

1. Set the TELNET server to Level 3 using the **WRKSRV** command

2. Use the **WRKTCPIPA** command to **enter the correct IP address**, then **enter the device name** to use for this IP address.

   You may also use a generic device name by putting an * at the end of the name. If you use a generic name, up to 99 will be used.

   For example:

   An entry of AP* would allow devices to be used as AP01 through AP99. The login process through TELNET will select the next available device name.

Setting the Required Password Type

This field must be set if the *TELNET Server* is set to Level 3. You must enter the appropriate setting for ALL TELNET IP address controls. As of OS/400 V4R2, only a setting of 0 or 1 is available. A setting of 2, although allowed here for encrypted passwords, is only available in V5R1 of OS/400.

Valid settings are:

0 – No password was received or validated

1 – A clear text password was received and validated

2 – An encrypted password was received (SSL TELNET only in V5R1)

- For normal TN5250 (TELNET support is VT100) you must set this to 0, since non-enhanced TELNET clients do not support this feature.

- For iSeries Access for Windows TELNET, you can use a setting of 1. However, certain iSeries Access for Windows clients do not support this, so you MUST test this at your location.

- A setting of 0 will always allow the client to connect.

Allow Auto Signon

1. Use the **WRKSRV** command to set the TELNET server to Level 3

2. Use the **WRKTCPIPA** *TELNET command **to enter the IP address** allowed for auto signon

3. **Enter the password type** (0 or 1 is required)

4. **Enter a Y** to allow auto signon

5. Use the **WRKSIGNON** command to **enter the IP address, the user profile, library, program or menu** that the client will automatically be signed on to.

For iSeries Access for Windows, you must set the TN5250 session parameters on the client setup to bypass signon (see the ISeries Access for Windows Setup Guide). This is required if you set the password type to 1 in the WRKTCPIPA setting.

For non-iSeries Access for Windows clients (named TELNET VT100 clients) you cannot use a password type of 1, only 0 is supported.

Important: If you intend to allow auto signon, please test this thoroughly, since it could present a security exposure.

Logging of TELNET Sessions

Under normal signon conditions (no auto signon allowed), each request for a TELNET session is logged into the transaction history file (TRAPOD) by IP address, and a user name of QSYS. QSYS is used because no user profile is associated with the actual TELNET session start request. Each logoff is also recorded by IP address with a user of QSYS.

If you use the auto signon feature, the request will be logged with the associated user set up in the Auto Signon Control file. Each logoff of a TELNET will also record the transaction with the user profile that was automatically signed on.

When *TELNETON is set to Level 3, only devices with IP addresses already registered will be permitted access to the TELNET server.

Changing the security level of the TELNET server functions takes effect immediately.

Setting up TCP/IP Address Controls

SafeNet/400 allows you to specify which client IP addresses are either accepted or rejected by the *Telnet* and the *FTP Servers*.

Turning on TCP/IP Address Checking

To set-up and turn on TCP/IP address checking for the **FTP Server** and **Rexec Server**

1. Type **WRKTCPIPA** *FTPSERVER then **ENTER**
2. Add the IP addresses to the Control Table
3. Type **CHGFTPSET** then press **F4**
4. Change *Server Source limit by IP Address?* to **YES* then **ENTER**
5. Use WRKSRV command and set the *FTPSERVER and/or *REXEC Server exit point to level 3 or 4.

To set-up and turn on TCP/IP address checking for the **FTP Client:**

1. Type **WRKTCPIPA** *FTPCLIENT then **ENTER**
2. Add the IP addresses to the Control Table
3. Type **CHGFTPSET** then press **F4**
4. Change *Client Target limit by IP Address?* to **YES* then **ENTER**
5. Use WRKSRV command and set the *FTPCLIENT exit point to level 3 or 4.

To set-up and turn on TCP/IP address checking for **TELNET:**

1. Type **WRKTCPIPA** *TELNET then **ENTER**
2. Add the IP addresses to the Control Table
3. Type **WRKSRV**
4. Change the **TELNETON* point to Level 3

Setting up TCP/IP Address Control Table

1. Use SafeNet/400 Main Menu *Option 7* or the **WRKTCPIPA** command

2. In *IP Addresses for Server* enter ***FTPSERVER, *FTPCLIENT** or ***TELNET** for the proper control table.

3. **Type the addresses to accept or reject**. **A** indicates Accept; **R** indicates Reject.

   Example 1:

Address	Accept/ Reject
10.2.2.X	A
10.2.2.5	R

   In this example any address from 10.2.2.1 through 10.2.2.255 will be accepted, with the exception of 10.2.2.5, which will be rejected.

   Example 2:

Address	Accept/ Reject
10.2.2.1XX	A
10.2.2.14X	R

   In this example all clients with addresses from 10.2.2.100 through 199 will be accepted, with the exception of clients addressed 10.2.2.140 through 10.2.2.149, which will be rejected.

To print the control table, select **Option 6 - Print TCP/IP Address Control Listing** on the SafeNet/400 Reports Menu.

Chapter 4 - SETTING UP FTP

Anonymous FTP Logon

To set up for Anonymous Logon, you must fill in the special FTP settings, and set the *FTP Logon Server* to Level 3 and the *FTP Server Validation* to Level 4.

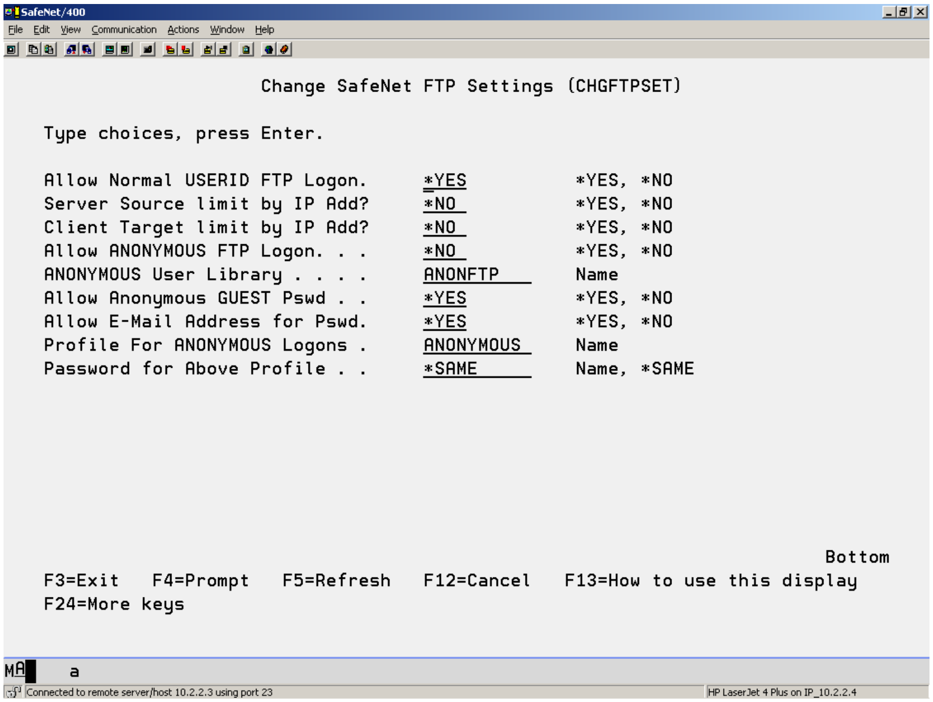
Follow these steps for FTP:

1. From the <u>SafeNet/400 Main Menu</u> select **Option 10 - Go to Special Jobs Menu**

2. From the <u>Special Jobs Menu</u> select **Option 3 - Change Special FTP Server Settings** or use **CHGFTPSET** command along with **F4**

   The *Change SafeNet FTP Settings* screen is displayed.

   Press F9 to see all parameters.


SafeNet/400
File Edit View Communication Actions Window Help
MA a
Connected to remote server/host 10.2.2.3 using port 23
HP LaserJet 4 Plus on IP_10.2.2.4

```
                       Change SafeNet FTP Settings (CHGFTPSET)

   Type choices, press Enter.

   Allow Normal USERID FTP Logon.     *YES          *YES, *NO
   Server Source limit by IP Add?     *NO           *YES, *NO
   Client Target limit by IP Add?     *NO           *YES, *NO
   Allow ANONYMOUS FTP Logon. . .     *NO           *YES, *NO
   ANONYMOUS User Library . . . .     ANONFTP       Name
   Allow Anonymous GUEST Pswd . .     *YES          *YES, *NO
   Allow E-Mail Address for Pswd.     *YES          *YES, *NO
   Profile For ANONYMOUS Logons .     ANONYMOUS     Name
   Password for Above Profile . .     *SAME         Name, *SAME

                                                                          Bottom
   F3=Exit   F4=Prompt   F5=Refresh   F12=Cancel   F13=How to use this display
   F24=More keys
```

Here you will find the special parameters to control login access to the *FTP Servers* from both Anonymous and regular user IDs.

Set the parameters for **CHGFTPSET** command as follows. The default value is highlighted in **bold**.

Parameter	**Screen Selections**	**Value**	**Description**
RLOGON	Allow Normal USERID FTP Logon	***YES** *NO	This parameter is used to determine whether or not you want regular OS/400 user Ids to be able to sign on through the FTP server. If you want only anonymous logons, set this to *NO and FTP for anonymous logons to *YES. If you say *NO to this option (allow normal System i5 user profiles to log on) then only anonymous logons will be allowed/disallowed based on the other parameters. Regular OS/400 user IDs will not be accepted for FTP logons.
IPCTL	Server Source limit by IP Add?	*YES ***NO**	To validate source IP addresses against a SafeNet/400 control table. Use **WRKTCPIPA *FTPSERVER**
IPCTLC	Client Target limit by IP Add?	*YES ***NO**	To validate Target IP addresses against a SafeNet/400 control table. Use **WRKTCPIPA *FTPCLIENT**
ALOGON	Allow Anonymous FTP Logon	*YES ***NO**	If you want users to be able to login with the user ID of Anonymous, enter *YES. If you don't want a user to use the FTP Logon User as Anonymous, leave this field *NO.
ALIBR	Anonymous User Library	*Libname*	When you allow anonymous logons, you must restrict those FTP users to a specific library. For security purposes, enter it here AND grant the user profile for anonymous logons object rights to this library or group of objects within this library from the SafeNet/400 Main Menu, *Option 3*. For the ANONYMOUS user profile under OS/400, make the 'Current Library' this library name. Also grant the anonymous user ID authority to the FTP server on the Main Menu, *Option 2*. Add the user to the valid FTP statements from the Main Menu, *Option 5*.

GUEST	Allow Anonymous GUEST Password	*YES ***NO**	To allow Anonymous user logins with the password of GUEST, enter ***YES** here. You can choose GUEST or use an E-mail address. *Note*: If you select GUEST, the System i5 still prompts an anonymous user for their E-mail address. **SafeNet/400**, however, will only allow GUEST as the password.
EMAIL	Allow E-mail Address for Password	***YES** *NO	If you allow an anonymous user to accept an E-Mail address, **SafeNet/400** will scan the address entered for an embedded “@” (at sign) for validation, and record the address in the log request file for reporting
AUSRPRF	Profile for Anonymous Logons	*profilename*	If you allow anonymous logons, you must specify a **<u>valid, pre-existing</u>** user profile to run anonymous user logons in OS/400 when the anonymous user logs on under FTP. In other words, a user would FTP to a System i5 FTP site running **SafeNet/400,** and that FTP site would prompt for a user name. The user keys ‘ANONYMOUS’ and the System i5 prompts for a password. The user then keys in a valid E-mail address and the System i5 starts a job assigned to the user ID you have specified here. The System i5 job is initiated using this profile and all its associated authorities. Enter the ANONYMOUS profile here, and if you want to assign a password to the profile enter that here also. **It is highly recommended that you leave this as *NONE, *NONE**. If you enter a password here, or use a profile other than ANONYMOUS, you leave a potential security exposure. ***Important:*** When using **SafeNet/400** and allowing for Anonymous, it is **strongly recommended that you create an OS/400 user profile called ‘ANONYMOUS’ with a**

			password of *NONE and *USER for the profile type. If you do this, no one can use this profile to sign on since the password is set to *NONE.
APWD	Password for Above Profile	*pword*	Enter the password to be used with the profile in parameter AUSRPRF for Anonymous FTP.

Setting up for ANONYMOUS FTP

Example

1. Create a user profile on the System i5 called ANONYMOUS, with password *NONE and user class *USER, and set the Current Library.

2. From the Special Jobs Menu, select **Option 3 - Change Special FTP Server Settings** or use **CHGFTPSET** command along with **F4**

3. Set the parameters as follows:

   - If you want to allow OS/400 users other than ANONYMOUS to log in through FTP server set parameter **RLOGON** to***YES**
   - Enter **ALOGON(*YES)** to allow ANONYMOUS
   - Enter **the library name** to which the user is restricted in parameter **ALIBR**
   - Enter **the type of password** you want the user to enter - E-mail or Guest, or both
   - Enter **the OS/400 user profile** in parameter **AUSRPRF** that was created in Step 1 above (ANONYMOUS)
   - Enter password for the ANONYMOUS user profile in **APWD** parameter

4. Press **ENTER**

5. Return to the SafeNet/400 Main Menu

6. Select **Option 1 - Work with Server Security Settings** or use **WRKSRV** command

7. Locate the *FTP Logon Server* point

8. Change the *FTP Logon Server* to Level 3

9. Change the *FTP Server Validation* point to Level 4. If you want to allow for anonymous logons, you **MUST** set this to Level 4

10. From the SafeNet/400 Main Menu, select **Option 2 -Work with User to Server Security** or use **WRKUSRSRV** command

11. Grant the ANONYMOUS user profile authority to the *FTP Logon* and *FTP Server Request Validation* server points.

12. From the SafeNet/400 Main Menu, select **Option 3 - Work with User to Object Level Security** or use **WRKUSROBJ** command

13. Grant the ANONYMOUS user authority to the library entered in step 3 above (Current Library), and specifically to any objects within the library. Or, enter *ALL for all object and then assign the required data rights.

If using long path support, use the **WRKUSRPTH** command to enter the correct path or paths for ANONYMOUS.

14. Select **Option 5 - Work with User to FTP Statement Security** or use the **WRKUSRFTP** command to grant the ANONYMOUS user ID authority to specific FTP commands. Use the additional FTP settings if required or if you want the ANONYMOUS profile initial path to be an IFS directory.

Setting up for Normal User IDs and FTP Servers

Example

1. From the <u>Special Jobs Menu</u> select **Option 3 - Change Special FTP Security Settings** or use **CHGFTPSET** command

2. On the <u>FTP Security Settings</u> screen, set *Allow normal user IDs to log on the FTP* to ***YES** or use **RLOGON (*YES)** parameter

3. Return to the <u>SafeNet/400 Main Menu</u> and select the following options:

   - Select **Option 1 - Work with Server Security Settings** or use **WRKSRV** command

     Locate the *FTP Logon, FTP Client* and/or *FTP Server* points. These must be set to Level 1, 3, 4. (If you set these to Level 1, you can skip the rest of these steps.)

   - Select **Option 2 - Work with User to Server Security** or use **WRKUSRSRV** command

     The user ID must be authorized to the *FTP Logon server* <u>and</u> one of the following:

     *FTP Client – if an OS/400 user will be FTP-ing OUT from your iSeries
     *FTP Server – if an OS/400 user will be FTP-ing INTO your iSeries

   - Select **Option 3 - Work with User to Object Level Security** or use **WRKUSROBJ** command

     Authorize the user ID to their own current library as specified in the OS/400 user profile. Enter this library in *User to Object Security*

     Authorize the user ID to any other library or object. Enter these in *User to Object Security*

   - Select **Option 5 - Work with User to FTP Statement Security** or use **WRKUSRFTP** command

     Authorize the user ID to the FTP statements they will use. Use **F4** for additional user settings if required.

   - Select **Option 6 - Work with User to CL Command Security**

     Authorize the user to the CL commands they will issue through the *FTP Server*

Chapter 5 - DHCP Controls and Reporting

Dynamic Host Configuration Protocol

DHCP allows clients to obtain IP network configuration, including an IP address, from a central DHCP server. DHCP servers control whether the addresses they provide to clients are allocated permanently or leased for a specific period of time. When the server allocates a leased license, the client must periodically check with the server to re-validate the address and renew the lease.

The DHCP client and server programs handle address allocation, leasing and lease renewal.

If you are using DHCP on your System i5 this gives you a way to control it. If you are not using DHCP, you can still use these options to review other activity.

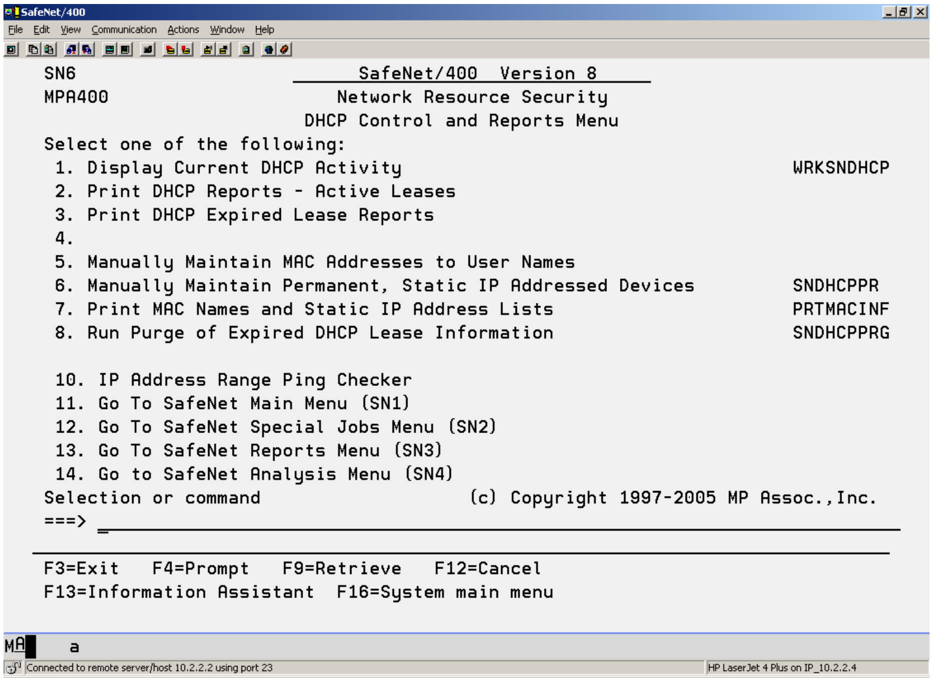
To use the System i5 as a DHCP server, refer to the relevant OS/400 manual and/or Operations Navigator.

Working with DHCP

DHCP functions are performed from the DHCP Control and Reports Menu.

From the SafeNet/400 Main Menu select **Option 13 – Go To DHCP Menu**

The *DHCP Control and Reports Menu* appears.



```
SN6                        SafeNet/400  Version 8
MPA400                       Network Resource Security
                            DHCP Control and Reports Menu
Select one of the following:
 1. Display Current DHCP Activity                                   WRKSNDHCP
 2. Print DHCP Reports - Active Leases
 3. Print DHCP Expired Lease Reports
 4.
 5. Manually Maintain MAC Addresses to User Names
 6. Manually Maintain Permanent, Static IP Addressed Devices        SNDHCPPR
 7. Print MAC Names and Static IP Address Lists                     PRTMACINF
 8. Run Purge of Expired DHCP Lease Information                     SNDHCPPRG

 10. IP Address Range Ping Checker
 11. Go To SafeNet Main Menu (SN1)
 12. Go To SafeNet Special Jobs Menu (SN2)
 13. Go To SafeNet Reports Menu (SN3)
 14. Go to SafeNet Analysis Menu (SN4)
Selection or command                    (c) Copyright 1997-2005 MP Assoc.,Inc.
===> _

F3=Exit   F4=Prompt   F9=Retrieve   F12=Cancel
F13=Information Assistant  F16=System main menu

MA     a
Connected to remote server/host 10.2.2.2 using port 23          HP LaserJet 4 Plus on IP_10.2.2.4
```

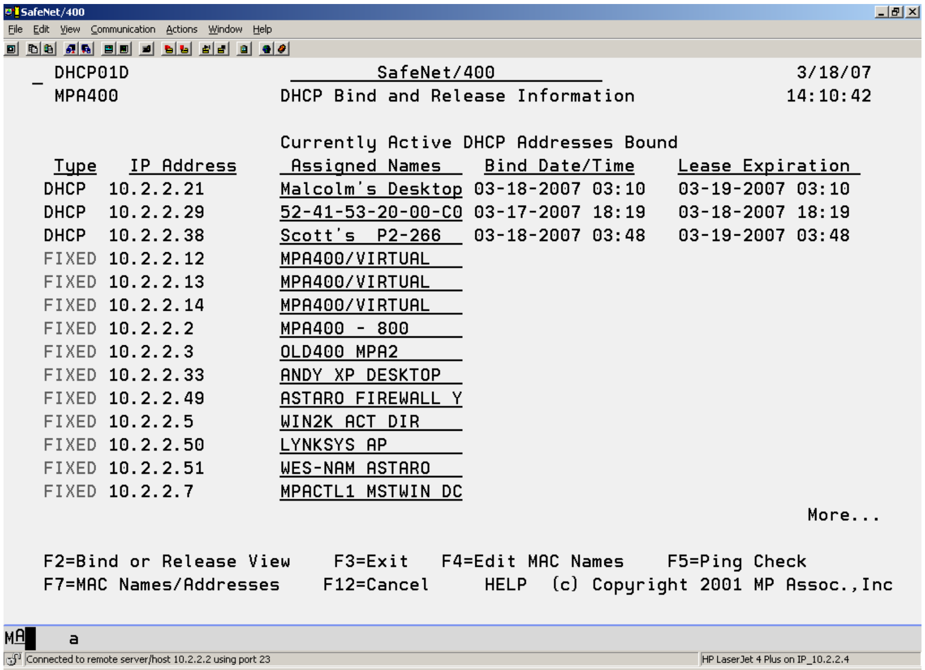
The DHCP functions provide the ability to maintain MAC addresses and device names, set IP addresses and ping IP addresses.

From the DHCP Control and Reports Menu you can also run reports for active and expired leases, MAC names and IP address lists.

Current DHCP Activity

To see current status, from the DHCP menu select **Option 1 – Display Current DHCP Activity**

This screen displays bind and release information



```
 _ DHCP01D                   SafeNet/400                            3/18/07
   MPA400               DHCP Bind and Release Information          14:10:42

                        Currently Active DHCP Addresses Bound
  Type   IP Address      Assigned Names    Bind Date/Time    Lease Expiration
  DHCP   10.2.2.21      Malcolm's Desktop 03-18-2007 03:10   03-19-2007 03:10
  DHCP   10.2.2.29      52-41-53-20-00-C0 03-17-2007 18:19   03-18-2007 18:19
  DHCP   10.2.2.38      Scott's  P2-266   03-18-2007 03:48   03-19-2007 03:48
  FIXED  10.2.2.12      MPA400/VIRTUAL
  FIXED  10.2.2.13      MPA400/VIRTUAL
  FIXED  10.2.2.14      MPA400/VIRTUAL
  FIXED  10.2.2.2       MPA400 - 800
  FIXED  10.2.2.3       OLD400 MPA2
  FIXED  10.2.2.33      ANDY XP DESKTOP
  FIXED  10.2.2.49      ASTARO FIREWALL Y
  FIXED  10.2.2.5       WIN2K ACT DIR
  FIXED  10.2.2.50      LYNKSYS AP
  FIXED  10.2.2.51      WES-NAM ASTARO
  FIXED  10.2.2.7       MPACTL1 MSTWIN DC
                                                                        More...

  F2=Bind or Release View    F3=Exit   F4=Edit MAC Names    F5=Ping Check
  F7=MAC Names/Addresses    F12=Cancel      HELP  (c) Copyright 2001 MP Assoc.,Inc

MA     a
Connected to remote server/host 10.2.2.2 using port 23          HP LaserJet 4 Plus on IP_10.2.2.4
```

Use function keys to switch views:

- F2 switches between the *Currently Active DHCP Addresses Bound* and *Expired or Released DHCP Addresses* screen

  The *Expired or Released* addresses list contains information gathered since the last time the list was purged.

- F7 switches between *MAC addresses* and the assigned names

  You will notice that the devices with fixed IP addresses do not change as you toggle between the two displays.

- F4 puts you in edit mode and allows you to revise the assigned names

Move your cursor to the name you want to change in the *Editable Names* column. Press **ENTER** to record the change.

To use this function make sure you are looking at the *Currently Active DHCP Addresses Bound* screen. Use F2 if necessary to switch.

- F5 pings the addresses

This will ping all the IP addresses that are displayed. The responses will flash at the bottom of the screen. When the process has completed, you will see a *Ping Status* column indicating the results of the pings.

If you are looking at the active addresses, you will ping those. If you are looking at expired or released addresses, all of those will be pinged.

Be aware that pinging the expired or released addresses can take a very long time depending on the last time the list was purged.

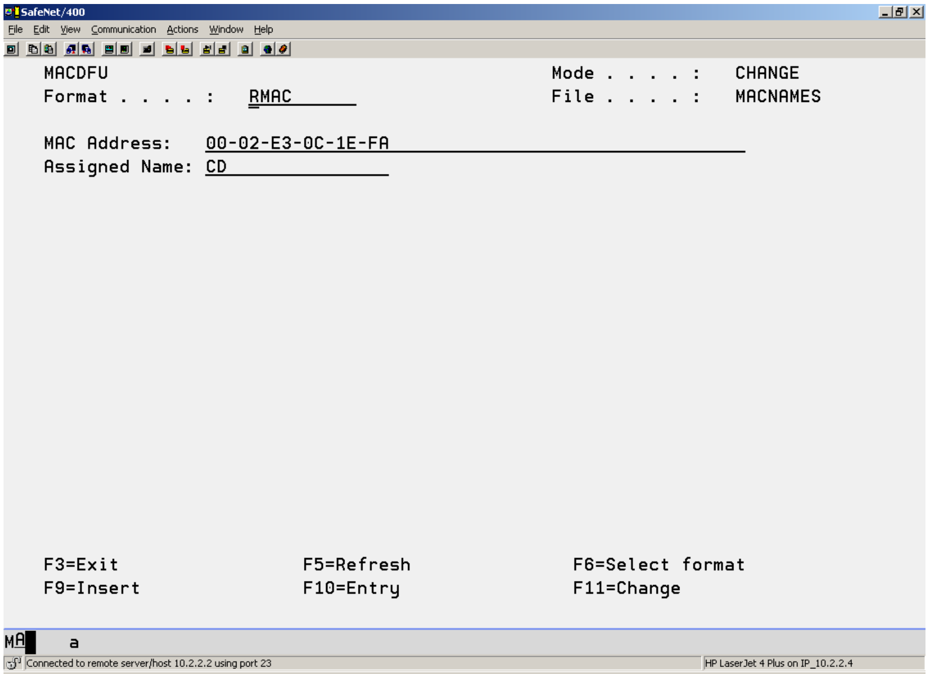
The number of packets and time to wait are controlled by two data areas: PINGPKTS and PINGTIME in PCSECDTA.

The default is one packet and one second wait. You can change these data areas manually if required.

Maintaining MAC Addresses

From the DHCP menu select **Option 5 – Manually Maintain MAC Addresses to User Names**

This operates as a standard OS/400 DFU program.



```
   MACDFU                                                      Mode . . . . :   CHANGE
   Format . . . . :   RMAC                                     File . . . . :   MACNAMES

   MAC Address:    00-02-E3-0C-1E-FA
   Assigned Name:  CD

   F3=Exit                     F5=Refresh                  F6=Select format
   F9=Insert                   F10=Entry                   F11=Change
MA     a
Connected to remote server/host 10.2.2.2 using port 23        HP LaserJet 4 Plus on IP_10.2.2.4
```

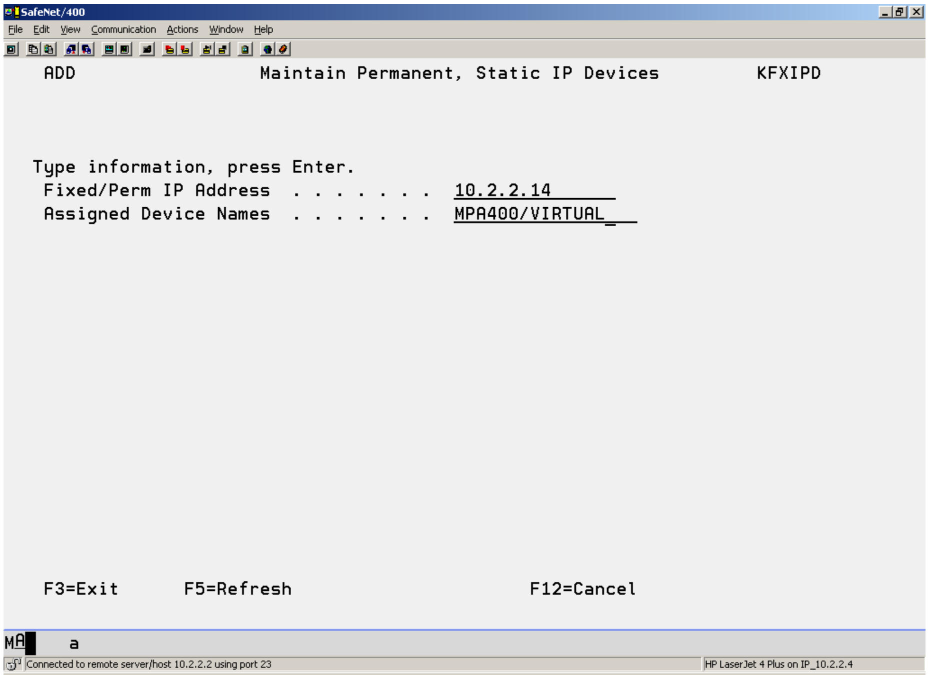
Press **F9** to use insert mode when editing

Press **F23** to delete the MAC address and name

Fixed IP Addresses

To assign IP addresses to devices, from the DHCP Menu select **Option 6 – Manually Maintain Permanent, Static IP Addressed Devices** or use the **SNDHCPPR** command

Even if you are not using DHCP on your System i5, you can use this option to do PING checks for network troubleshooting.



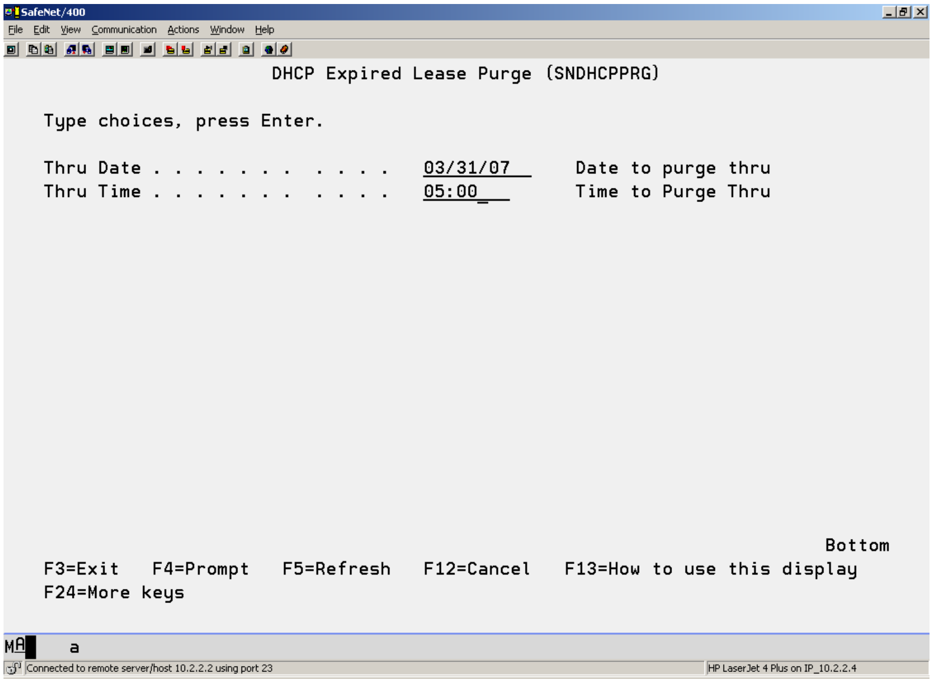
```
   ADD                  Maintain Permanent, Static IP Devices        KFXIPD


  Type information, press Enter.
   Fixed/Perm IP Address  . . . . . . .  10.2.2.14______
   Assigned Device Names  . . . . . . .  MPA400/VIRTUAL___


   F3=Exit      F5=Refresh                     F12=Cancel
MA     a
Connected to remote server/host 10.2.2.2 using port 23        HP LaserJet 4 Plus on IP_10.2.2.4
```

If you enter a DHCP IP address you will receive an error message. This is for fixed IP addresses only.

Purging Expired DHCP Lease Information

The *Expired or Released DHCP* address information is cumulative and will remain in the system until you purge it.

From the DHCP Menu select **Option 8 – Run Purge of Expired DHCP Lease Information**



SafeNet/400
File Edit View Communication Actions Window Help

```
                     DHCP Expired Lease Purge (SNDHCPPRG)

   Type choices, press Enter.

   Thru Date . . . . . . . .  . . . .   03/31/07__    Date to purge thru
   Thru Time . . . . . . . .  . . . .   05:00___      Time to Purge Thru

                                                                     Bottom
   F3=Exit   F4=Prompt   F5=Refresh   F12=Cancel   F13=How to use this display
   F24=More keys
```

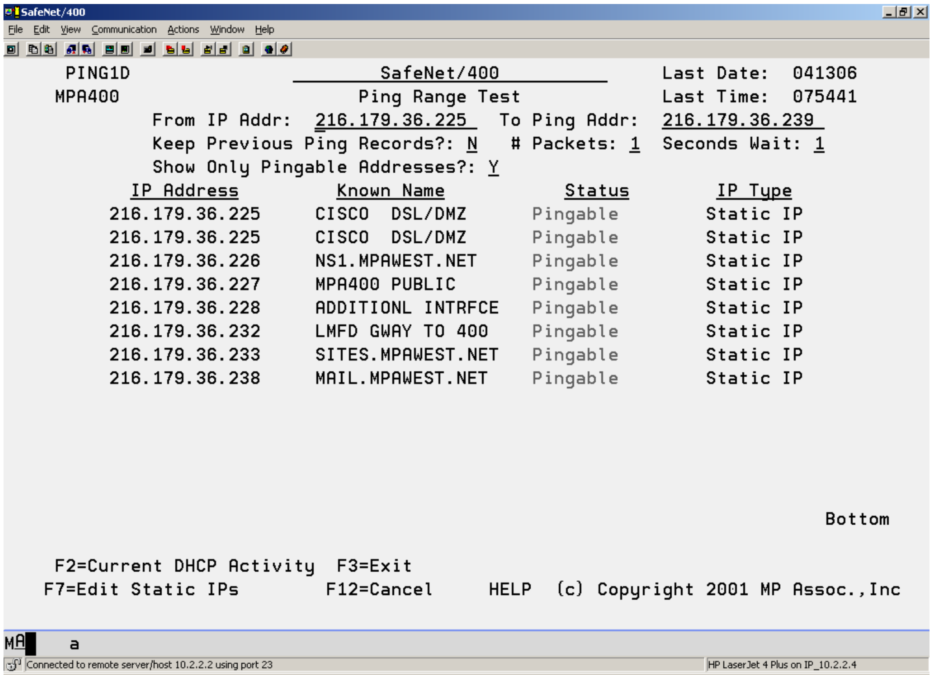
MA   a
Connected to remote server/host 10.2.2.2 using port 23
HP LaserJet 4 Plus on IP_10.2.2.4

Enter the date and time to purge through. When you **ENTER** the log of expired DHCP leases will be cleared.

Ping Checker

You can use this option to ping a single IP address or a range of addresses.

From the DHCP Menu select **Option 10 – IP Address Range Ping Checker**



```
     PING1D                     SafeNet/400                 Last Date:  041306
    MPA400                     Ping Range Test              Last Time:  075441
             From IP Addr:  216.179.36.225   To Ping Addr:  216.179.36.239
             Keep Previous Ping Records?: N   # Packets: 1   Seconds Wait: 1
             Show Only Pingable Addresses?: Y
           IP Address          Known Name          Status         IP Type
         216.179.36.225     CISCO  DSL/DMZ      Pingable        Static IP
         216.179.36.225     CISCO  DSL/DMZ      Pingable        Static IP
         216.179.36.226     NS1.MPAWEST.NET     Pingable        Static IP
         216.179.36.227     MPA400 PUBLIC       Pingable        Static IP
         216.179.36.228     ADDITIONL INTRFCE   Pingable        Static IP
         216.179.36.232     LMFD GWAY TO 400    Pingable        Static IP
         216.179.36.233     SITES.MPAWEST.NET   Pingable        Static IP
         216.179.36.238     MAIL.MPAWEST.NET    Pingable        Static IP




                                                                         Bottom

    F2=Current DHCP Activity  F3=Exit
   F7=Edit Static IPs        F12=Cancel     HELP  (c) Copyright 2001 MP Assoc.,Inc

MA     a
Connected to remote server/host 10.2.2.2 using port 23          HP LaserJet 4 Plus on IP_10.2.2.4
```

Enter the range of IP addresses that you want to ping.

Press **ENTER** and you will begin to see replies flash on the bottom of the screen.

When all the IP addresses have been pinged the *Status* column will display the results of the pings.

Chapter 6 - REPORTS

SafeNet/400 reports are grouped into two categories:

- **Setup Reports** provide information on server settings, user authorities to servers and to data, etc.

- **Analysis Reports** provide data on **SafeNet/400** usage - the who, what, where and when information you need to manage your system.

  Analysis reports have been enhanced to include the ability to select specific dates and/or users, including summaries by group profile. You can choose to print the reports or create an OUTFILE of the selected records in a readable format to use for your own ad-hoc reporting.

  You can also use the analysis reports to take advantage of the Auto-enrollment feature of **SafeNet/400**. See the SafeNet/400 Implementation Guide for more information.

Setup Reports

These reports are accessed through the SafeNet/400 Main Menu, *Option 11 – Go to Setup Reports Menu* (**GO SN3** command)

1. Server Status

Prints each Server Function and its security level setting

2. User to Server Security Listing

Lists users and the Server Functions they are authorized to

3. User to Object Security Listing

Lists users, the libraries and objects they have authority to and the rights the users have to the objects.

4. User to SQL Statement Listing

Lists all users and the SQL statements they are authorized to use

5. User to FTP Statement Listing

Lists all users and the FTP statements they are authorized to use

6. TCP/IP Address Control Listing

Lists the TCP/IP address controls for Workstation Gateway and FTP servers.

7. User to CL Command Listing

Lists users and the CL commands they are authorized to use

8. User to Long Path Security Listing

Lists users and long path names they are authorized to use

Usage Reports

These reports are accessed through the SafeNet/400 Main Menu, *Option 12 – Go to Analysis Reports Menu* (**GO SN4** command).

Menu SN4 options 2 through 7 also give you the ability to run auto-enrollment reports and perform the auto-enrollment process.

1. Security Report by User (Also Batch Transaction Test Report)

Lists each request by user, the Server Functions they are requesting, the server's security level setting, and whether the request was accepted or rejected.

Can also be used as a test report to recheck all historical transactions against current and future **SafeNet/400** settings.

Allows "what if" testing of all historical transactions against current and future control file settings to see if further set up is required.

2. User to Server Usage Report

Using historical transactions, lists each server a user has accessed

3. User to Object Usage Report

Using historical transactions, lists each LIB/OBJ a user has accessed and the type of access, i.e., READ, WRITE, DELETE.

4. User to SQL Usage Report

From historical transactions, lists each SQL operation performed by each user.

5. User to FTP Usage Report

From historical transactions, lists each FTP operation performed by each user.

6. User to CL Command Usage Report

Using historical transactions, lists each CL command issued by each user.

7. User to IFS Path Usage Report

Using historical transactions, lists each path accessed by each user.

Chapter 7 - TESTING YOUR SECURITY SETTINGS

Once you have planned your server function Security Level settings, **SafeNet/400** gives you a method to test the settings to make sure they will provide the level of security you anticipate. It acts as a “what-if” tool to verify the effect your settings will have before you actually turn on access control.

If you have been logging network requests with **SafeNet/400** you can, at any time, run each historical record through the security checking routines and receive a result of ‘ACCEPTED’ or ‘REJECTED’ based on current and future **SafeNet/400** settings.

This allows you to make changes to the server function Security Level, the user-to-server settings, or data rights authorities, and using previously logged requests, tell immediately if your settings will give the desired response to the clients.

To test your collected transactions use:

- *On-line Transaction Tester* (PCTESTR) – the preferred method
- *Security Report by User* in test mode (Menu SN4, *Option 1*)

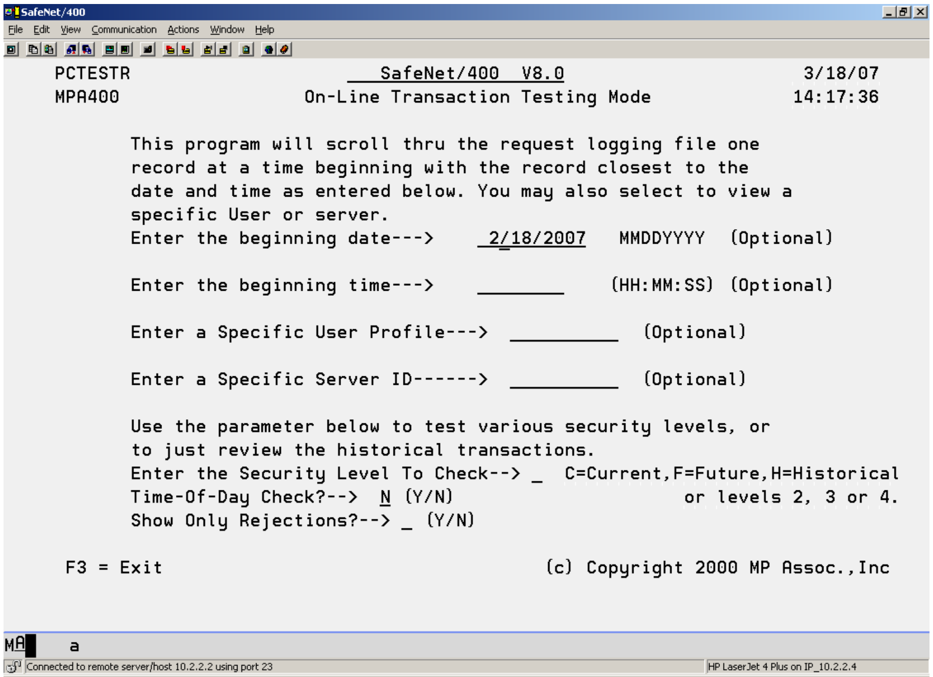
Testing SafeNet/400 settings based on your historical data with the on-line transaction tester

This is the preferred method if you would like immediate feedback.

1. From the SafeNet/400 Main Menu select **Option 10 - Go to Special Jobs/Setup Menu** or use **GO SN2** command**)**

2. Select **Option 10 - On-Line Transaction Testing** or use **PCTESTR** command

   The *On-Line Transaction Testing* screen will appear.



```
    PCTESTR                     ___SafeNet/400  V8.0                    3/18/07
    MPA400                 On-Line Transaction Testing Mode            14:17:36

           This program will scroll thru the request logging file one
           record at a time beginning with the record closest to the
           date and time as entered below. You may also select to view a
           specific User or server.
           Enter the beginning date--->    _2/18/2007   MMDDYYYY  (Optional)

           Enter the beginning time--->    ________    (HH:MM:SS) (Optional)

           Enter a Specific User Profile---> __________  (Optional)

           Enter a Specific Server ID------> __________  (Optional)

           Use the parameter below to test various security levels, or
           to just review the historical transactions.
           Enter the Security Level To Check--> _  C=Current,F=Future,H=Historical
           Time-Of-Day Check?--> N (Y/N)                        or levels 2, 3 or 4.
           Show Only Rejections?--> _ (Y/N)

     F3 = Exit                                   (c) Copyright 2000 MP Assoc.,Inc

MA      a
Connected to remote server/host 10.2.2.2 using port 23        HP LaserJet 4 Plus on IP_10.2.2.4
```

If you want, you may enter a beginning date and time, or the user or server ID, then enter the desired security level to test against your logged transactions.

If you do not enter a date and time, you will be shown requests beginning with the first available record in the file.

3. In the *Security Levels to Check* field:

   Type C (Current) to test transactions with your **present SafeNet/400** Server Security Levels

   Type H (Historical) to review the actual status received when the transaction was logged; no new ‘re-testing’ is performed.

   Type F (Future) to test transactions with your **future** Server Security Levels. This will test each selected transaction against the future security setting to determine if your security control files are set up correctly.

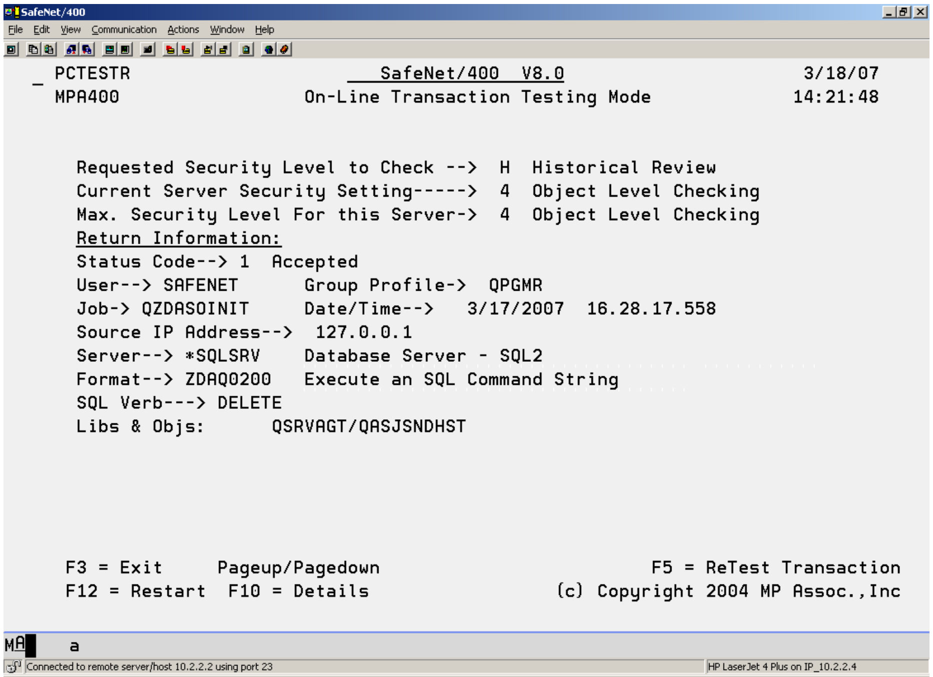
   Type 2, 3 or **4** for other levels

   If you want to test your Time-of-Day controls, **type Y** in Time of Day Check.

   If you want to see only rejected requests, **type Y** in *Show only Rejections*.

Important: If you elect to display only rejections, be advised that this may seriously impact interactive performance. Consider using the *Batch Transaction Test Report* as an alternative.

4. When you press **ENTER** and a transaction that meets your selection criteria is found, the *On-Line Transaction Testing Mode* screen is displayed.



```
 _ PCTESTR                    SafeNet/400  V8.0                      3/18/07
   MPA400                On-Line Transaction Testing Mode           14:21:48


     Requested Security Level to Check -->  H  Historical Review
     Current Server Security Setting----->  4  Object Level Checking
     Max. Security Level For this Server->  4  Object Level Checking
     Return Information:
     Status Code--> 1  Accepted
     User--> SAFENET      Group Profile->  QPGMR
     Job-> QZDASOINIT     Date/Time-->   3/17/2007  16.28.17.558
     Source IP Address-->  127.0.0.1
     Server--> *SQLSRV    Database Server - SQL2
     Format--> ZDAQ0200   Execute an SQL Command String
     SQL Verb---> DELETE
     Libs & Objs:      QSRVAGT/QASJSNDHST





    F3 = Exit     Pageup/Pagedown                        F5 = ReTest Transaction
    F12 = Restart  F10 = Details               (c) Copyright 2004 MP Assoc.,Inc

MA      a
```

Connected to remote server/host 10.2.2.2 using port 23

HP LaserJet 4 Plus on IP_10.2.2.4

This describes:

- The Requested Security Level setting to check
- The current Security Level for the server
- The maximum security level setting for this server
- The user making the request
- The group profile related to the user
- The date and time of the request
- The OS/400 server job name the request came from
- The format
- The server function receiving the request
- Data used, if any
- Whether the request was accepted or rejected, and the reason for the rejection

- If it is displayed as a valid function key, you can **press F10** to view even more detail.

- Additional command keys are shown when rejections are displayed. These additional command keys will allow you to work directly with the appropriate user setting based on the rejection code.

5. You can roll up or down to scroll backward and forward, or you can press **ENTER** to scroll forward to the next record in the logging file.

   At any time you can press **F12** to return and enter a new starting date and time, server or user, or change the Security Level to check.

Note: Use this tool to develop and test your initial security settings prior to putting them into production. You can go back and change the different **SafeNet/400** parameters to see how they affect each transaction.

Use the additional command keys shown in rejections to immediately make changes to user settings.

Batch Transaction Test Review/Report – Security Report by User

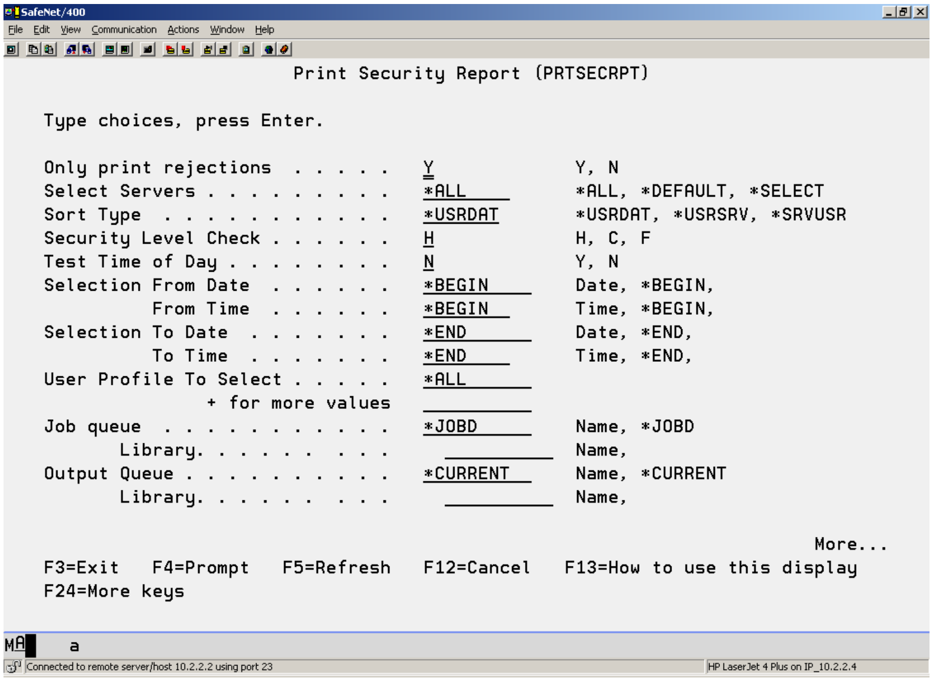
You can use this batch report to test all the historical transactions through current and future control file settings.

With this report you can make changes to control files, then re-run all the historical transactions back through a security check process to determine if further security set up is required.

If you want to see the same servers each time you run this security report, you can customize it by using Special Jobs Menu *Option 1 - Select Default Servers for Security Report*. This option lets you select the specific servers you are interested in, then makes them the default each time you run the report.

Run this report from Menu SN4, the Network Transaction Analysis Reports Menu *Option 1 - Print Security Report by User* or use the **PRTSECRPT** command.

Use F9 to display all parameters



```
                    Print Security Report (PRTSECRPT)

 Type choices, press Enter.

 Only print rejections  . . . . .   Y              Y, N
 Select Servers . . . . . . . . .   *ALL           *ALL, *DEFAULT, *SELECT
 Sort Type  . . . . . . . . . . .   *USRDAT        *USRDAT, *USRSRV, *SRVUSR
 Security Level Check . . . . . .   H              H, C, F
 Test Time of Day . . . . . . . .   N              Y, N
 Selection From Date  . . . . . .   *BEGIN         Date, *BEGIN,
           From Time  . . . . . .   *BEGIN         Time, *BEGIN,
 Selection To Date  . . . . . . .   *END           Date, *END,
           To Time  . . . . . . .   *END           Time, *END,
 User Profile To Select . . . . .   *ALL
                + for more values
 Job queue  . . . . . . . . . . .   *JOBD          Name, *JOBD
        Library. . . . . . . . .                   Name,
 Output Queue . . . . . . . . . .   *CURRENT       Name, *CURRENT
        Library. . . . . . . . .                   Name,

                                                              More...
 F3=Exit   F4=Prompt   F5=Refresh   F12=Cancel   F13=How to use this display
 F24=More keys

MA    a
Connected to remote server/host 10.2.2.2 using port 23      HP LaserJet 4 Plus on IP_10.2.2.4
```

On the *Print Security Report screen* fill in the following*:*

1. Decide if you wish to print all transactions or only those that were rejected.
   Enter Y for only rejections (the default) or **N** to print all transactions

   Printing only rejections will reduce the size of the output report

2. Select the servers to include in the report

    - ***ALL** - all servers
    - ***DEFAULT** - based on servers that were selected on Menu SN2, *Option 1 - Select Default Servers for Security Report*
    - ***SELECT** - displays a list of servers to choose from

3. Select your preferred *Sort Type*

    - ***USRDAT** - by user, then by date within user
    - ***USRSRV** - by user, then by server within user
    - ***SRVUSR** - by server, then by user within server

4. Select the correct *Security Level Check* value

    - **H** = Historical Review only

      Show status at actual time of client request

    - **C** = Check all transactions against current server settings
    - **F** = Check all transactions against the *Future* server settings

5. Decide if you want to test the time of day controls

    Enter **Y** or **N** for the *Test Time of Day* parameter

6. Select these optional parameters

    - Enter a start date and time or accept the default value
    - Enter an ending date and time or accept the default value
    - Enter a specific user ID or *ALL

Page Down if you would like to print the report to an output file.

When you have finished making your selections, **ENTER** to submit the report to batch.

Recommended approach to testing

A recommended approach to using the *On-Line Transaction Testing* program is:

1. Set all of the important server functions to Security Level 1, Log All. This will log all requests without affecting any users. Set your *Future Server* settings or use the pre-loaded recommended values.

   Turn off logging on the non-critical servers to limit logging.

2. Collect your requests and print out the *Security Report by User* from the Network Transaction Analysis Reports Menu. Select *Historical Review*.

3. Set up your *User to Server* and *User to Object, SQL, FTP, CL,* etc. tables if you wish to go to Security Level 4.

4. You can use several tools provided with **SafeNet/400** to test your security settings. Use the *Security Report by User* or the on-line version, *PCTESTR*. These can be run to test the collected transactions against the current or future server settings. (Use Future Setting)

5. Use ‘Show only Rejections’ on PCTESTR and ‘Print only Rejections’ on the batch report. If your settings are correct for the Security Levels being tested, you should receive messages only for transactions that would be rejected.

   If any of the requests are rejected, check the message description and make the appropriate corrections to the **SafeNet/400** settings. Try the transaction again.

Note: If you request Level 4, you may only get a security check to Level 3 since some servers support only up to Level 3. This is noted on each record in the *On-Line Transaction Testing* as “Level Requested”, “Level Checked” and “Max Level”.

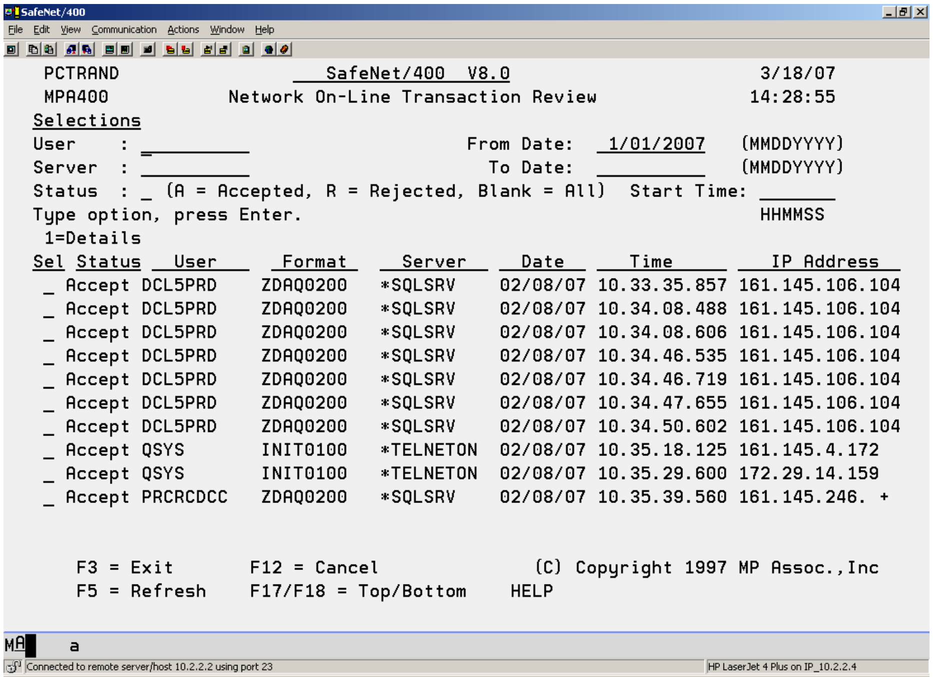
PCREVIEW

Use the **PCREVIEW** command or **Option 9 - On-Line Transaction Review** from the SafeNet/400 Special Jobs Menu to review each transaction logged by **SafeNet/400**.

This displays the historical transactions only. No testing can be performed using this tool.

1. Type **PCREVIEW** and press **ENTER**.

   The *Network On-Line Transaction Review* screen is displayed and the **HELP** key is active.



```
   PCTRAND                    SafeNet/400  V8.0                      3/18/07
   MPA400           Network On-Line Transaction Review              14:28:55
  Selections
  User    : __________                 From Date:  1/01/2007   (MMDDYYYY)
  Server  : __________                   To Date:  __________  (MMDDYYYY)
  Status  : _ (A = Accepted, R = Rejected, Blank = All)  Start Time: _______
  Type option, press Enter.                                          HHMMSS
   1=Details
  Sel Status  User      Format    Server     Date    Time         IP Address
   _ Accept DCL5PRD    ZDAQ0200   *SQLSRV    02/08/07 10.33.35.857 161.145.106.104
   _ Accept DCL5PRD    ZDAQ0200   *SQLSRV    02/08/07 10.34.08.488 161.145.106.104
   _ Accept DCL5PRD    ZDAQ0200   *SQLSRV    02/08/07 10.34.08.606 161.145.106.104
   _ Accept DCL5PRD    ZDAQ0200   *SQLSRV    02/08/07 10.34.46.535 161.145.106.104
   _ Accept DCL5PRD    ZDAQ0200   *SQLSRV    02/08/07 10.34.46.719 161.145.106.104
   _ Accept DCL5PRD    ZDAQ0200   *SQLSRV    02/08/07 10.34.47.655 161.145.106.104
   _ Accept DCL5PRD    ZDAQ0200   *SQLSRV    02/08/07 10.34.50.602 161.145.106.104
   _ Accept QSYS       INIT0100   *TELNETON  02/08/07 10.35.18.125 161.145.4.172
   _ Accept QSYS       INIT0100   *TELNETON  02/08/07 10.35.29.600 172.29.14.159
   _ Accept PRCRCDCC   ZDAQ0200   *SQLSRV    02/08/07 10.35.39.560 161.145.246. +


      F3 = Exit       F12 = Cancel            (C) Copyright 1997 MP Assoc.,Inc
      F5 = Refresh    F17/F18 = Top/Bottom    HELP

MA      a
Connected to remote server/host 10.2.2.2 using port 23          HP LaserJet 4 Plus on IP_10.2.2.4
```

2. Using the fields at the top of the screen, you can select only the records you wish displayed. You can select by user, server, status, from and to date.

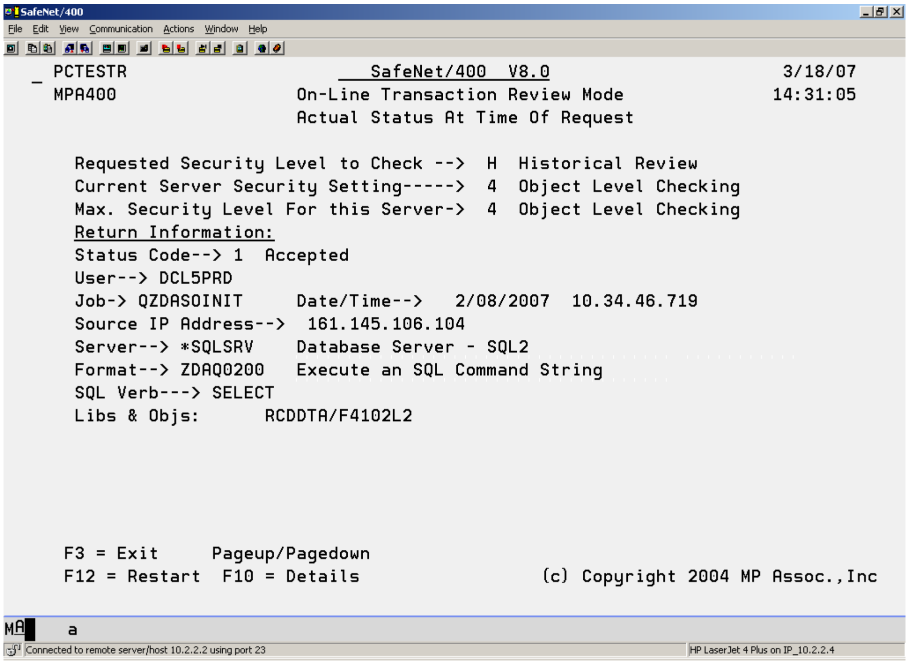
   For example, to review only rejections for today:

   - **Type R** in the Status field

   - By default, today's date is entered for you

3. To obtain additional information about a particular record, **type a 1** next to the record and press **ENTER**.

The *On-Line Transaction Review Mode* screen is displayed, supplying more detailed information about the specific transaction.



```
 _ PCTESTR                    ___SafeNet/400  V8.0                      3/18/07
   MPA400                 On-Line Transaction Review Mode              14:31:05
                          Actual Status At Time Of Request

     Requested Security Level to Check -->  H  Historical Review
     Current Server Security Setting----->  4  Object Level Checking
     Max. Security Level For this Server->  4  Object Level Checking
     Return Information:
     Status Code--> 1  Accepted
     User--> DCL5PRD
     Job-> QZDASOINIT     Date/Time-->   2/08/2007  10.34.46.719
     Source IP Address-->  161.145.106.104
     Server--> *SQLSRV    Database Server - SQL2
     Format--> ZDAQ0200   Execute an SQL Command String
     SQL Verb---> SELECT
     Libs & Objs:      RCDDTA/F4102L2





    F3 = Exit     Pageup/Pagedown
    F12 = Restart  F10 = Details                (c) Copyright 2004 MP Assoc.,Inc

MA     a
```

Connected to remote server/host 10.2.2.2 using port 23
HP LaserJet 4 Plus on IP_10.2.2.4

You can use the **ROLL UP/ROLL DOWN** keys to scroll through the sequential transactions or **press ENTER** to return to the PCREVIEW sub-file screen.

If you selected only a specific user or server to be displayed in PCREVIEW, you will find that only those records meeting the selection criteria will be displayed as you scroll through the file with the on-line transaction test program.

Chapter 8 - BACKUPS AND PURGES

Log file Purge

When **SafeNet/400** is logging client requests, the information is kept in the TRAPOD file in library PCSECDTA. At times this file may grow to a considerable size. This function deletes the records in the TRAPOD file.

There are two ways to purge the TRAPOD file:

1. Standard purge using retention days or purge-through date

2. Archive TRAPOD records and generate a report

   This allows you to specify the number of days to retain records or a purge-through date, and provides the capability to archive the records to an alternate file and member. You can also print a report listing either all of the purged records or only those records that were rejections.

To perform a standard purge

1. Backup the TRAPOD file to tape, if desired. You will need to issue the **ENDTRP** command **<u>BEFORE</u>** beginning the backup.

2. Select **Option 8** from the <u>Special Jobs Menu</u> or use the **STRPRG** command.

3. Enter **the number of days** to retain information in the TRAPOD file or **enter the date** to purge through. The default is to retain the information for thirty days.

4. You can direct the processing of the purge to a specific job queue.

   If you leave the default value of *JOBD, then the default job queue for your job will be used.

   If you choose to use a different job queue, you can enter the name here. You must have the job queue's library name in your job's library list when you use this option.

5. If you ended logging prior to performing a backup, issue the **STRTRP** command to restart logging.

You can use the following command instead of the menu option:

```
STRPRG DAYS(060)
```

This will purge the TRAPOD file and retain 60 days of data. The number of days must be entered as three characters, i.e., 020 for 20 days.

To purge the log and archive the records

1. Select **Option 8** from the Special Jobs Menu or use the **STRPRGARC** command.
2. Enter **the number of days** to retain information in the TRAPOD file or **enter the date** to purge through. The default is to retain the information for thirty days.
3. Make sure *Archive purged records* is set to ***YES**
4. Set *Print purged records* and *Only print rejections* to whichever option you wish
5. Use **F10** to display *Additional Parameters*
6. Select ***YES** or ***NO** for *Remove deleted records*

   ***YES** requires that transaction logging be turned off

You can use the following command instead of the menu option:

```
STRPRGARC DAYS(060) ARC(*YES) PRT(*YES) PRTR(*NO) RMVDEL(*NO)
```

This will purge the TRAPOD file and retain 60 days of data; archive the records; print a report listing all records, not just rejections.

All archived records are transferred to a file named TRAPARCW in PCSECDTA. Each time the archive command is run, a new file member is added to this file. It is recommended that for auditing purposes you save the archive file to tape, then remove the members.

Automating the log file purge

To automatically purge the log file, archive the purged records and generate the transaction report, use the following command or add it to the system job scheduler:

```
SBMJOB CMD(PCSECLIB/STRPRGARC DAYS(XXX)  JOB(SECPRG)
```

XXX is the number of days to retain records (060 = 60 days retention)

Automating the One Step Security Report

To automatically run the security report without purging or archiving any records, use the following command:

```
PRTSECRPT
```

There are no parameters for this command

To submit this command to batch type:

```
SBMJOB CMD(PCSECLIB/PRTSECRPT)
```

For additional selection criteria for this report, use menu SN4, the Network Transaction Analysis Reports menu, *Option 1 - Print Security Report by User*.

Automating and Running the Security Report and the Log File Purge Together

Use this method to automate both the **SafeNet/400** *Security Report* and the *Log File Purge.*

For this example, the purge is being done on Mondays and Thursdays. You may use any schedule you wish; however, make sure your purge is retaining enough days for reporting purposes.

Each of these commands provides parameters to print either only rejections or all transactions. Review these parameters and change as required.

<u>Monday</u>

1. Run purge and retain 5 days, print report of all rejected, purged records

    STRPRGARC DAYS(005)

2. Run security report - it will print rejections for the last 5 days (Thursday through Monday)

    PRTSECRPT

<u>Thursday</u>

1. Run purge and retain 4 days, print purged rejected records

    STRPRGARC DAYS(004)

2. Run security report - it will print rejections for the last 4 days (Monday through Thursday)

    PRTSECRPT

This example runs the Log File Purge and retains only 1 day of data in the file.

Saturday

1. Run security report and see entire contents of log

   PRTSECRPT

2. Run purge and retain 1 day

   STRPRGARC DAYS(001)

Note: It is a good idea to run these commands back-to-back and at off-peak hours to minimize performance impact.

Daily Backup Procedure

Modify your daily backup procedure to follow these guidelines:

1. Enter command **CHGSPCSET LOGALL(*NO)**

   This prevents **SafeNet/400** from attempting to log requests

2. Issue the **ENDTRP** command within **SafeNet/400**

   This will end the transaction logging program and subsystem

3. Perform your normal backup steps

4. **CHGSPCSET LOGALL(*YES)** to begin logging

5. Issue the **STRTRP** command to re-start the transaction logging subsystem and program

Remember to include the **SafeNet/400** data library, PCSECDTA in your daily backup procedure.

Chapter 9 - DE-ACTIVATING AND REMOVING SAFENET/400

You must be signed on as a Super Admin in SafeNet/400 to perform any Activate/De-Activate processes. See 'SafeNet Administrator' in Chapter One of this guide.

De-activating SafeNet/400

Under some circumstances you may want to de-activate **SafeNet/400**. It may be necessary when troubleshooting network problems to make sure they are not being caused by an application such as **SafeNet/400**, or when you need to remove **SafeNet/400** from your system.

If after you have de-activated **SafeNet/400** you still have problems with network requests or connections, you may want to IPL your System i5 or **ENDSBS *ALL** to uncover any autostart jobs or other IPL-initiated OS/400 activities that may still be allocating **SafeNet/400** objects and programs. This is not required if you do not need to de-allocate all the **SafeNet/400** programs.

Once you have been successful in isolating your network problem, you can re-activate **SafeNet/400**.

Before de-activating

Optionally, rather than de-activating SafeNet/400 you can remove one or more exit points if required.

For example, if you have a problem with the *FILESRV server function use the **WRKREGINF** command to:

1. Locate the OS/400 exit point for the *FILESRV server function
2. Remove the **SafeNet/400** exit program
3. Stop and restart the file server

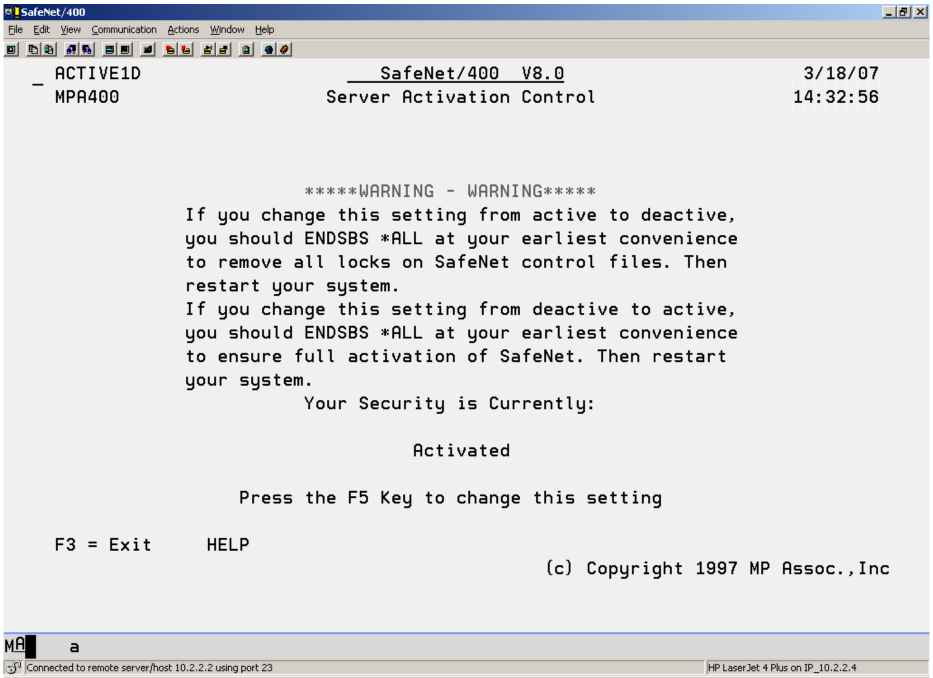
This will prevent the OS/400 file server job from using **SafeNet/400** but continue to protect the other server jobs in OS/400 with **SafeNet/400**. This way you can eliminate a performance problem or OS/400 problem from one server but continue to protect your other access points with **SafeNet/400**.

To activate or de-activate SafeNet/400:

Remember, you must be a **SafeNet/400** Super Admin to perform this step.

1. From the Special Jobs Menu select **Option 6 - Activate/De-Activate SafeNet/400**

   The *Server Activation Control* screen is displayed, indicating the current setting.



```
 _  ACTIVE1D                     SafeNet/400  V8.0                    3/18/07
    MPA400                   Server Activation Control              14:32:56


                           *****WARNING - WARNING*****
                 If you change this setting from active to deactive,
                 you should ENDSBS *ALL at your earliest convenience
                 to remove all locks on SafeNet control files. Then
                 restart your system.
                 If you change this setting from deactive to active,
                 you should ENDSBS *ALL at your earliest convenience
                 to ensure full activation of SafeNet. Then restart
                 your system.
                            Your Security is Currently:

                                      Activated

                      Press the F5 Key to change this setting

    F3 = Exit     HELP
                                                 (c) Copyright 1997 MP Assoc.,Inc

MA     a
Connected to remote server/host 10.2.2.2 using port 23          HP LaserJet 4 Plus on IP_10.2.2.4
```

2. **Press F5** to change the setting and return to the Special Jobs Menu.

3. After performing these steps, end all subsystems then restart them to maintain security integrity.

4. Try your network request again. If **SafeNet/400** is active, and your request is not successful, review your request log and correct the problem based on the error code on the report.

Removing SafeNet/400 from your system

If it becomes necessary to completely remove **SafeNet/400** from your System i5, follow these steps.

1. Sign on to the System i5 as QSECOFR or SAFENET.

2. De-activate **SafeNet/400**.

   Follow the instructions on the previous pages to de-activate the program.

3. IPL the System i5.

4. Delete library PCSECLIB and PCSECDTA

5. Delete the SAFENET authorization list from your system

   SafeNet/400 is now completely removed from your system.

Chapter 10 - PROBLEM DETERMINATION

If **SafeNet/400** is not working properly, there are a few general things to check.

Error Message Received on the System i5

1. Did you perform an IPL after the initial **SafeNet/400** installation?

   It is necessary to IPL your System i5 after completing the installation steps. If you do not IPL your system, you will experience unpredictable results.

   Recovery: IPL your system then try **SafeNet/400** again.

2. Is the PTF level on your System i5 current?

   Compare your PTF level with **SafeNet/400** required levels.

   Recovery: Install the latest cumulative PTF package if necessary.

3. Is your client application current on service packs or fixes?

   Check to make sure you have the most recent level of fixes for your client.

   Recovery: Apply latest service pack or fix package

4. Is this the first time you are using this client application?

   If this is the first time you are using this particular application, it may be that your server functions are not set up properly.

   Recovery: Check **SafeNet/400** request logs for errors and correct. Use on-line testing program to verify your settings are correct.

5. Have you made changes to server function Security Levels or user authority tables?

   If a particular request was working, and now it is not, make sure you have not inadvertently disabled a server function or revoked authorities from a user.

   Recovery: Double check changes against the request log, use the on-line transaction program to test your authority settings.

Error Message Received on the Client

If you receive an error message indicating a problem with a client or a communications request, or an exit program rejection and **SafeNet/400** is active:

Check the request log for a ‘REJECTED’ response

1. Use the date and time along with the user ID to find the request that was rejected. Use **PCREVIEW** or check the Security Report.

2. When you find the request that was rejected, the log will indicate the reason for the rejection. You will find a list of error codes and their descriptions at the end of this chapter.

3. If you need to make changes to authorities you can test your changes with the on-line transaction program before you implement them. See Chapter 7 in this guide, ‘Testing your Security Settings.’

If the request does not appear in the log or the Review screen

These steps should help you determine if the problem is network related, client related or **SafeNet/400** related.

1. Try the same request with a user ID that has rights to all servers and has all object and all folder authority. User profile QSECOFR is set up with all rights in **SafeNet/400** by default.

2. Check the log file for the request and response.

3. Make changes to authorities if necessary.

4. Try the request again with the original client or with the on-line transaction program.

5. Try a different client or user ID.

If you are unsure that SafeNet/400 is the source of the problem

1. Reset the Security Level in **SafeNet/400** by following these directions:

   - From the SafeNet/400 Main Menu select **Option 1 – Work with Server Security Settings** or use **WRKSRV** command

   - If you know which server function the request is using, change the server's Security Level to 1. If you cannot determine which server function the request is attempting to access, set all the servers to Security Level 1.

   - Try the client request again

   - If the request is successful, change the server (or servers) back to the original Security Level, Logging Level All. This will log all the client requests.

2. Try the client request again.

   - If the request is successful, run the request log report and review the client request.

   - If the request is rejected, check PCREVIEW to view the actual transaction.

   - Make the required authority table changes. Test your changes with the on-line transaction program.

   - Try the client request again and review the logs again.

If you receive a message on the System i5 about a **SafeNet/400** or PCSECLIB program, or you still cannot resolve a client error or client application error, check to see if the system was IPL'd since you:

- Initially installed **SafeNet/400**

- Applied PTFs to **SafeNet/400**

If not, you must IPL your system for the changes to take effect.

If you still cannot resolve the problem

1. Check all the joblogs for the jobs in the subsystems:

   QSYSWRK
   QSERVER

2. You may have to change the QDFTJOBD job description to capture the joblogs of certain jobs initiated by client requests.

   ```
   CHGJOBD  QDFTJOBD  LOGLVL(4 00 *SECLVL)  LOGCLPGM(*YES)
   ```

   Note: Remember to change this back to its default when you have resolved the problem or you may generate an excessive number of joblogs.

   ```
   CHGJOBD  QDFTJOBD  LOGLVL(4 00 *NOLIST)  LOGCLPGM(*NO)
   ```

3. End then start both subsystems:

   QSYSWRK
   QSERVER

4. Try the client request again

5. Check for joblogs and errors

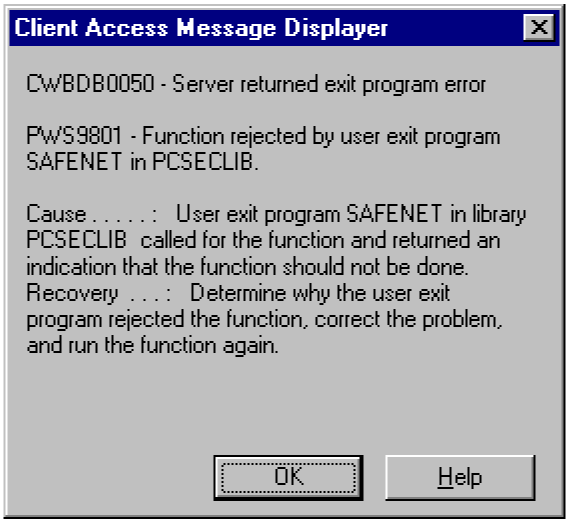
6. You may have to end and re-start QSYSWRK and QSERVER to force joblog creation.

   Also try **ENDTCPSVR *ALL, ENDHOSTSVR *ALL;** then **STRTCP** and **STRHOSTSVR *ALL.**

To determine if the problem is with the server or a client, try this process with another client application that may access the same server.

Examples of Client Error Messages

Some common error messages you may see on a Windows95 client:

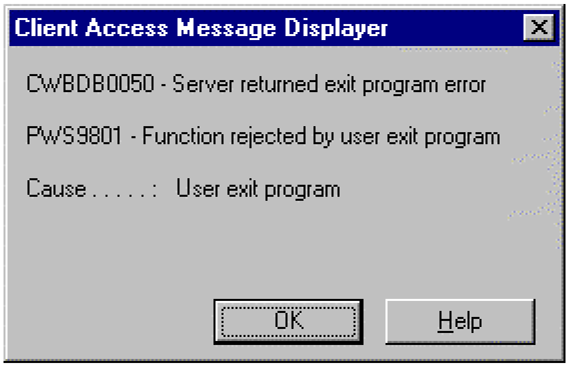


CWBDB0050 - Server returned exit program error

PWS9801 - Function rejected by user exit program SAFENET in PCSECLIB.

Cause . . . . . : User exit program SAFENET in library PCSECLIB called for the function and returned an indication that the function should not be done.
Recovery . . . : Determine why the user exit program rejected the function, correct the problem, and run the function again.

This message was received on the client when the server function was set to Level 2 - Function Disabled/No Access.

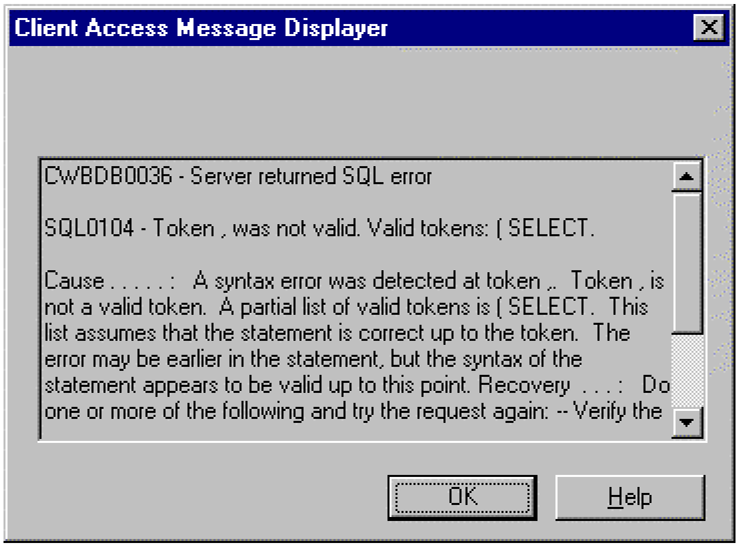


CWBDB0050 - Server returned exit program error

PWS9801 - Function rejected by user exit program

Cause . . . . . : User exit program

This message was received on the client when the user was not authorized to the server.



CWBDB0036 - Server returned SQL error

SQL0104 - Token , was not valid. Valid tokens: (SELECT.

Cause . . . . . : A syntax error was detected at token ,. Token , is not a valid token. A partial list of valid tokens is (SELECT. This list assumes that the statement is correct up to the token. The error may be earlier in the statement, but the syntax of the statement appears to be valid up to this point. Recovery . . . : Do one or more of the following and try the request again: -- Verify the

This message was received on the client when the user was not authorized to the SQL Select statement.

Error Codes which Appear in the Log

1	Accepted	
0	Rejected	Reason unavailable
A	Rejected	Server is turned off
B	Rejected	No authority to server
C	Rejected	No authority to object
D	Rejected	No authority to library
E	Rejected	Invalid Data Rights authority
F	Rejected	Invalid Object Management Rights
G	Rejected	Unauthorized path statement
H	Rejected	No authority to SQL statement
I	Rejected	Incoming commands *OFF
J	Rejected	No authority to Root Directory
K	Rejected	Unauthorized FTP Logon
L	Rejected	Unauthorized FTP Command
N	Rejected	Unauthorized REXEC Logon
O	Rejected	Unauthorized TFTP Logon
P	Rejected	Unauthorized IP Address
Q	Rejected	Invalid Op-Specific Request

R	Rejected	Auto-signon requires password
S	Rejected	TELNET requires password
T	Rejected	Encrypted password required
U	Rejected	No devices available
V	Rejected	Unauthorized CL command
X	Rejected	Error with Swap Profile
Y	Rejected	Error during Profile Swap
Z	Rejected	User/Server Reject Code (Specific *REJECT in WRKUSRSRV)
@	Rejected	Time of Day control
#	Rejected	Function requires SafeNet/400 regular Admin authority
$	Rejected	Function requires SafeNet/400 Super Admin authority

Additional Troubleshooting Tips

PCREVIEW Command

Use the PCREVIEW commands to easily view historical network transactions. You can select various filters to display only the records from the log file you are interested in. From this screen you can request details of the information.

TRAPOD File

When testing network requests through **SafeNet/400** you can see each transaction being written to the **TRAPOD** file in library PCSECLIB.

Use the OS/400 DSPPFM (Display Physical File Member) command to look at the contents of the **TRAPOD** file. Type **B** on the *Control line* and press **ENTER**. This will take you directly to the bottom of the file and enable you to see the last request recorded in the file.

As a network request is processed by **SafeNet/400**, a record is written to the **TRAPOD** file. The name of the **SafeNet/400** program that processed the request is in position 1-10; the status of the request is in position 11 (1= Accepted, all others are rejections); the user profile is in position 12-21.

The rest of the record contains specific information based on the request type. Detailed information is available in IBM's TCP/IP Configuration and Reference Guide or the specific licensed program manual.

Chapter 11 - SPECIAL SAFENET/400 CONSIDERATIONS

This section contains information on procedures that will help you manage and automate certain **SafeNet/400** functions.

Resetting Level 5 within SafeNet/400

When an installation has a user exit program in place that **SafeNet/400** does not recognize, the exit point will automatically be set to Level 5 (unsupported). To allow **SafeNet/400** to support this server you must do the following:

1. Remove your user exit program from the registration facility in OS/400.

   Type WRKREGINF and press **ENTER**

   Locate the exit point and remove your exit program.

   Important: Do not remove any program called from PCSECLIB.

   You may have several servers set to Level 5. You must remove each one. Then, using the DSPNETA or CHGNETA command, verify that the System i5 network attributes DDMACC and PCSACC are both set to *OBJAUT.

   If these attributes are not initially set to *OBJAUT, **SafeNet/400** will flag several exit points to Level 5.

2. Type the following:

   CALL PCSECLIB/DELST5CL and press **ENTER**

3. From the SafeNet/400 Main Menu select **Option 1 - Work with Server Security Settings** or use **WRKSRV** command.

   Press F3 to exit **without making any changes**

4. Using the System i5 console, you must place the system in a restricted state with the **ENDSBS *ALL *IMMED** command, or any other site-specific shutdown process.

5. De-activate **SafeNet/400**

   From the Special Jobs Menu select **Option 6 - Activate/De-Activate SafeNet/400**

Follow the instructions to de-activate the program found in Chapter 9 in this guide, 'De-activating and Removing SafeNet/400'.

6. Re-activate **SafeNet/400**

   Select **Option 6 - Activate/De-Activate SafeNet/400**

7. Restart your system

Pre-Power Down Program Point

You can create a power down CL program to be called whenever the PWRDWNSYS command is issued. **SafeNet/400** will call this program and log the request whenever the command is processed.

To use this feature, create a CL program called PWRDWNCL and place it in library QGPL.

Using Automatic Alert Notification

Alert notification continually monitors network activity and can issue warning messages to up to five different message queues whenever an attempt is made to access an unauthorized server or object.

You can also choose to have alerts sent via e-mail. This uses the **SNDDST** command and requires that you set up a distribution list. When creating a distribution list for alert notification, the List ID Qualifier **MUST** be your System i5 system name.

In addition, you must have set up SMTP mail options on the System i5.

There are two types of alert notification available. We recommend using summarized alerts after the initial installation and setup. Using summarized alerts, you can prevent a flood of e-mails in the event of a large number of rejected transactions being processed by SafeNet/400.

1. Summarized alerts - you can receive a message that gives summarized information regarding **SafeNet/400** rejections. For example, "There have been six (6) rejections by **SafeNet/400** since 01/01/99 at 12:00:00".

   This process starts the SAFELOGING subsystem**,** which contains a pre-start job called ALERTWATCH. SAFELOGING runs from the *BASE memory pool and uses very little system resources. You can set the time interval between alerts; by default 30 minutes is used.

   When you specify summary alerts via e-mail, **SafeNet/400** will include a list of the summarized alerts in the form of an e-mail attachment text file.

2. Detailed alerts - you can specify that **SafeNet/400** send detailed alert messages. Every **SafeNet/400** rejection will generate a message that describes the user, server and date/time that a request was rejected.

   This option does not start the ALERTWATCH program, since it is not required when detailed messages are specified.

   Use detailed message alerts when you initially set up SafeNet/400. This will allow you to quickly get an alert in the event of rejections that may need additional research and set up.

Activating SafeNet/400 Alert Notification

1. From the SafeNet/400 Special Jobs Menu select **Option 7 - Change Alert Notification Status** or use the **CHGNOTIFY** command and **press F4**.

2. **Type *ON** for parameter *ALERT* to activate alert notification, then **ENTER.**

3. Enter ***YES** to receive summarized alerts or ***NO** for detailed alerts.

4. Enter ***YES** to receive alerts as e-mail or ***NO** to receive alerts as workstation messages only.

   Your system must be configured for SMTP before e-mails can be used.

5. **Enter the message queue(s) and/or e-mail distribution list(s)** that should receive these alerts. You can send alerts to both message queues and distribution lists.

   The alerts are not sent to message queues in *BREAK mode. To receive these alerts immediately, make sure the user message queue is in *BREAK mode. (See CHGMSGQ command in the IBM CL Manual)

6. You can enter **individual e-mail addresses** to receive alerts in addition to, or instead of, message queues and distribution lists.

   Use the '+' sign to enter additional values.

7. Press ENTER to display the parameter to set the **Summarized Alert Interval**

   If the *Summarized Alerts* parameter is set to ***YES**, you can specify the number of minutes between alerts. You will receive notification when each interval expires, indicating the number of rejections since the last notification.

Creating a Distribution List

Use the CRTDSTL command to create a distribution lists for SafeNet/400 alerts.

Profile Swapping

Profile Swapping allows you to assign an alternate or a "swapped" user profile to be interrogated by **SafeNet/400** and passed to OS/400 for security lookups.

When profile swapping is in use, any incoming network transactions or jobs are assigned the alternate profile (the 'Swap to' profile) and passed as this alternate profile to OS/400. OS/400 then performs all security related checking as if the request came from the 'Swap to' profile and not the original profile. The job in OS/400 retains its original user name.

All authority checking by **SafeNet/400** is performed using the original profile name.

Alternate Profile Swapping is controlled using the **CHGSPCSET** command (**SafeNet/400** Menu SN2, *Option 2*). Set the *SWAPU* parameter to one of these values:

- ***NO**

  Do not swap profiles within **SafeNet/400**

- ***OPT**

  SafeNet/400 will swap profiles if the original user has an alternate swap profile set up in **SafeNet/400**

- ***RQD**

  Requires that a swap profile must be set up for the original profile in **SafeNet/400**, or all requests are rejected.

Setting up a Swap Profile

Make sure that you have set the *SWAPU* parameter on the **CHGSPCSET** command to allow profile swapping. Then follow these steps to set up your alternate profiles.

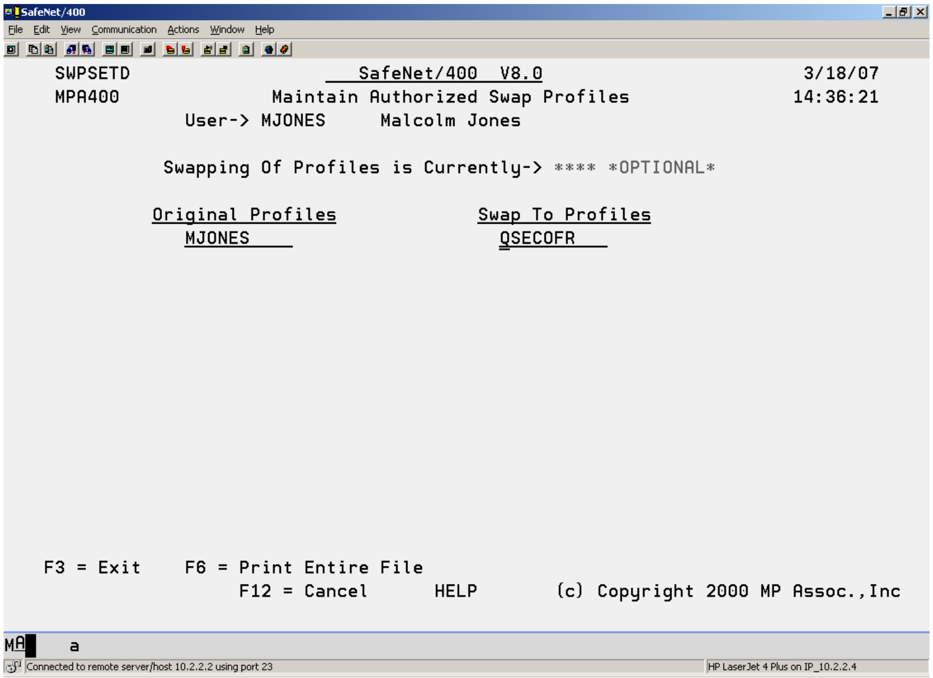
1. From the <u>Special Jobs Menu</u>, select *Option 15 - Swap Profile Maintenance* or use the WRKSWPPRF command

2. Enter the **user profile** to work with.

   You can type the user profile, use F4 for a list, or type *ALL for a complete list of swap profiles.

   Press **ENTER**

   The *Maintain Authorized Swap Profiles* screen appears



```
   SWPSETD                       SafeNet/400  V8.0                   3/18/07
   MPA400             Maintain Authorized Swap Profiles             14:36:21
               User-> MJONES     Malcolm Jones

             Swapping Of Profiles is Currently-> **** *OPTIONAL*

              Original Profiles            Swap To Profiles
                 MJONES                       QSECOFR



  F3 = Exit    F6 = Print Entire File
                    F12 = Cancel      HELP       (c) Copyright 2000 MP Assoc.,Inc

MA    a
Connected to remote server/host 10.2.2.2 using port 23          HP LaserJet 4 Plus on IP_10.2.2.4
```

3. On the Maintain Authorized Swap Profiles screen, **type the *Swap To Profile*** then press **ENTER**

Now, whenever a user connects to the System i5 through a client/server connection after **SafeNet/400** checks the original profile, OS/400 will do all security checking on the ‘Swap to’ profile.

Journaling SafeNet/400 Security Files

You may wish to journal all changes made to any of the **SafeNet/400** security files for audit purposes. Three programs are provided to assist with the journaling process:

1. Call PCSECLIB/STRSAFEJRN

    - Creates all required journals (SAFENET) in library PCSECLIB
    - Creates journal receiver (SAFE1) in library PCSECLIB
    - Starts journaling on eleven SafeNet/400 control files

2. Call PCSECLIB/ENDSAFEJRN

    - Stops journaling on the eleven SafeNet/400 control files

3. Call PCSECLIB/DLTSAFEJRN

    - Deletes all associates journals and journal receivers

Note: Options 2 and 3 (END and DELETE) require a dedicated System i5 and must be performed from the system console while the System i5 is in a restricted state.

Although at this time we have not provided any reporting programs for the **SafeNet/400** journals, we intend to make that report available as a PTF at a future date.

Files Contained in SafeNet/400

These files are available for you to use for any additional reporting requirements you may have. All are located in library PCSECDTA.

DHCPBLOG

Contains DHCP Bindings log reports

DHCPRLOG

Contains DHCP Release log reports

ERRORD File

Contains all error codes (accepted/rejected) associated with **SafeNet/400**.

FIXEDIPS

Contains fixed IP client addresses (static addresses)

IBMFLR File and **IBMFLRL** (Long paths to IBM folders)

Contains all IBM supplied folder names. You may add additional folder names to this file for automatic READ and/or WRITE authority as required.

MACNAMES

Contains MAC addresses with names of associated clients

TRAPARCW File

Contains all the purged transactions if the STRPRGARC command was utilized.

TRAPOD File

All logged network requests are placed in this file. This file will grow significantly over time, depending on network traffic. Be sure to pay close attention to its size and establish a schedule to purge records.

This file can also be used for additional user-developed reporting. See IBM OS/400 Servers and Administration for additional information and record layouts.

SafeNet/400 Commands

Commands	**Description**
ADDSNADM	Maintain SafeNet administrators
ADDSNUSR	Allows batch maintenance of SafeNet/400 users
ADDUSRCMD	Allows batch maintenance of users to commands
ADDUSRFTP	Allows batch maintenance of users to FTP
ADDUSROBJ	Allows batch maintenance of users to objects
ADDUSRSQL	Allows batch maintenance of users to SQL
ADDUSRSVR	Allows batch maintenance of users to servers
CHGFTPSET	Change FTP special settings
CHGNOTIFY	Changes status of Alert Notification
CHGSPCSET	Change SafeNet/400 special settings
CPYSNUSR	Copy settings from one SafeNet/400 user to another
ENDTRP	Ends the transaction logging program
PCREVIEW	Starts the on-line transaction review process
PCTESTR	Starts the on-line transaction testing program
PRTCLUSG	Reports command usage and auto-enrollment
PRTFTPUSG	Starts the FTP transaction and testing program
PRTOBJUSG	Starts the object transaction and testing program
PRTPTHUSG	Starts the IFS path transaction and testing program
PRTSECRPT	Print security report

Commands	Description
PRTSQLUSG	Reports SQL statement usage and auto-enrollment
PRTSRVUSG	Reports server usage and auto-enrollment
RMVSNUSR	Removes a user from all SafeNet/400 enrollments
RMVSNUSR1	Removes all profiles not defined to OS400. Excludes profiles Beginning with ‘*’ (*Public)
RMVUSRCMD	Removes user’s authorities to CL commands
RMVUSRFTP	Removes user’s authorities to FTP
RMVUSROBJ	Removes user’s authorities to objects
RMVUSRSQL	Removes user’s authorities to SQL
RMVUSRSRV	Removes user’s authorities to server functions
SETSAFENET	OPTION(A) – Activates SafeNet/400
SETSAFENET	OPTION(B) – Deactivates SafeNet/400
SETVER	Used to change the license code level of SafeNet/400
STRALRT	Starts Alert Notification monitoring
STRPRG	Starts purge of log file
STRPRGARC	Starts archive purge/security report of log file
STRTRP	Starts the transaction logging program and SBS
WRKSIGNON	Work with TELNET signon parameters
WRKSNADM	Maintain SafeNet/400 Administrators
WRKSNSUSR	Work with SafeNet/400 Super Users
WRKSNDHCP	Work with current DHCP activity
WRKSRV	Work with server security settings

Commands	**Description**
WRKSWPPRT	Work with Swap Profiles
WRKTCPIPA	Work with TCP/IP address control
WRKUSRCMD	Work with user to CL commands
WRKUSRFTP	Work with user to object FTP statement security
WRKUSROBJ	Work with user to object security
WRKUSRPTH	Work with User to IFS path security
WRKUSRSEC	Work with user security. Permits access to all security screens for an individual user without entering several different commands.
WRKUSRSQL	Work with user to object SQL statement security
WRKUSRSRV	Work with user to server security

Chapter 12 - SERVER FUNCTION DESCRIPTIONS

This section lists all the current System i5 server functions, their descriptions and information on how they are used. The servers are alphabetized within two groups - the **Original Servers** and the **Optimized Servers**.

Original Servers

These servers have been provided by IBM since PC Support/400 became available. Support for these original servers was designed for and is still used to service the original clients: DOS, Extended DOS and OS/2.

Distributed Data Management

Description: Distributed Data Management - 100

Security checking is performed when a remote user or system accesses a System i5 file or issues an incoming remote command via DDM. The remote user must be authorized to perform the operation (open, close, read or write, for example) or the DDM request is rejected.

Where used:	iSeries Access for Windows Client Access for Windows 3.1 Client Access for OS/2 Client Access for DOS with Extended Memory Client Access for DOS System i5 to System i5, System/38™ or System/36™ Communication	
Server Identifier:	*DDM	
Format Name:	*DDM	
Levels Supported:	Basic	(Levels 1,2,)
	Intermediate	(Level 3)
	Advanced	(Level 4)
	Plus special setting for remote command processing CL command authority checking is performed at Level 4	
Limitations:	- See the Special Jobs Menu for incoming remote commands - Cannot check authority of files, objects or commands imbedded in the command string	
Recommended Setting:	Level 4, Log All	

Notes:

1. Commands are allowed only if specified from Special Jobs Menu, *Option 2* (**CHGSPCSET** command). DDM commands, NOT file requests, can be stopped by saying "NO" to *Allow DDM Commands* parameter. The **SafeNet/400** default is "YES" to allow commands. Review existing requirements prior to changing this setting. At Level 4, users must be authorized to commands.

2. Does not support *SPC type transactions.

3. For Version 4 of **SafeNet/400**, if *DDM is set to Level 4, you must authorize each user to the CL commands they may issue to the System i5.

4. Most System i5 systems, by default, use the QUSER profile for the communications conversation. QUSER must have authority to all files that are being accessed and must be authorized to the *DDM server function.

   To change from QUSER as the default, a change to the default communications entry must be made in the QCMN subsystem description. See your system administrator for assistance.

Original Data Queue Server

Description: Original Data Queue Server - 100

A data queue is a System i5 object that is used by System i5 application programs for communications. Applications can use data queues to pass data between jobs. Multiple System i5 jobs can send or receive data from a single data queue.

Where used:	Client Access for Windows 3.1 Client Access for OS/2 Client Access for DOS with Extended Memory Client Access for DOS	
Server Identifier:	*DQSRV	
Format Name:	DTAQ0100	
Levels Supported:	Basic	(Levels 1,2)
	Intermediate	(Level 3)
	Advanced	(Level 4)
Limitations:	None	
Recommended Setting:	Level 1, Log All	

Notes:

1. At Levels 3 and 4 users must be granted access to the server function.

2. At Level 4 users must be granted access to specific data queues and libraries.

3. Supports generic (wildcard) data queue names. (DATAQ* = all data queue names starting with the letters DATAQ)

Original Transfer Function Server

Description: Original File Transfer Function - 100

The Client Access transfer function transfers data between the System i5 system and a personal computer.

Where used: Client Access for Windows95
- *PC5250 Transfers*
- *Automatic file transfer functions (RTOPCB, etc.)*

Client Access for Windows 3.1
- *Interactive and automatic file transfer functions*
- *File transfer from within a RUMBA** emulation session*

Client Access for OS/2
- *Interactive and automatic file transfer functions*
- *File transfer from within a RUMBA emulation session*

Client Access for DOS with Extended Memory
- *Interactive and automatic file transfer functions*
- *File transfer from within a RUMBA or PC5250* emulation session*

Client Access for DOS
- *Interactive and automatic file transfer functions*

Server Identifier: *TFRFCL

Format Name: TRAN0100

Levels Supported:	Basic	(Levels 1,2)
	Intermediate	(Level 3)
	Advanced	(Level 4)

Recommended Setting: Level 4, Log All

Notes:

1. Specific users must be granted access to the server function at Levels 3 and 4.

2. Users must be granted access to specific files and libraries at Level 4.

3. Supports generic (wildcard) file names. (FI* = all file names starting with the letters FI)

4. Full control of library, object and data rights allowed.

5. At Level 4, to select or extract a list of objects from within a library, you must enter the name of the library and use *ALL in the *Object or Sub-Flr* column. The user will need Read data rights to the library.

   Example 1: To get a list of all files in *USRLIBL there must be an entry for the user requesting the list:

Library or Folder	Object or Sub-Folder	Read
*USRLIBL	*ALL	X

   Example 2: To get a list of all files in the library PAYROLL enter:

Library or Folder	Object or Sub-Folder	Read
*PAYROLL	*ALL	X

6. CRTFILE(*YES) CRTMBR(*YES)

   To do a “REPLACE” with a CREATE FILE(*YES) or a CREATE MEMBER(*YES), Existence Rights must be given to the user for the FILE/LIBRARY being created.

   To do a “REPLACE” with a CREATE FILE(*NO) or CREATE MEMBER(*NO), Delete and Write Data Rights must be specified to the object.

Original License Management Server

Description: Original License Management Server - 100

The license management server ensures valid licenses are available for Client Access, IBM and non-IBM licensed applications when requested from a client. The license management server performs this process every time a Client Access client requests a license for an application, typically upon session initiation. When a Client Access client disconnects from the System i5, the license is released and is available for another client to use.

Where used: Client Access for Windows 3.1
Client Access for OS/2
Client Access for DOS with Extended Memory
Client Access for DOS

Server Identifier: *LMSRV

Format Name: LICM0100

Levels Supported: Basic (Levels 1,2)
Intermediate (Level 3)

Limitations: None

Recommended Setting: Level 1, Log All

Notes:

1. At Level 3 the user must be authorized to the server function.

2. Level 4 is not required or supported.

Original Message Server

Description: Original Message Server - 100

The message function server allows users to communicate with each other by sending messages. Users can communicate with other users at System i5 workstations or with users at personal computers that are attached to the System i5 system.

The message function server routes messages sent from PC users to the appropriate user and receives messages for PC users and sends them to the PC workstation.

Where used: Client Access for OS/2
Client Access for DOS with Extended Memory
Client Access for DOS

Server Identifier: *MSGFCL

Format Name: MESS0100

Levels Supported: Basic (Levels 1,2)
Intermediate (Level 3)

Limitations: None

Recommended Setting: Level 1, Log All

Notes:

1. At Levels 3 and 4, the user must be authorized to the server function.

2. Generic (wildcard) names are supported for Level 4.

Original Remote SQL Server

Description: Original Remote SQL Server - 100

The remote SQL server processes requests that are received from Client Access products that are using the high-level language remote SQL API. The API allows applications running on the clients to run SQL statements on a remote System i5 system. The databases accessed may be either SQL database files or native System i5 database files.

Where used:	Client Access for Windows 3.1 Client Access for OS/2 Client Access for DOS with Extended Memory Client Access for DOS	
Server Identifier:	*RQSRV	
Format Name:	RSQL0100	
Levels Supported:	Basic	(Levels 1,2)
	Intermediate	(Level 3)
	Advanced	(Level 4)
Limitations:	ODBC support on Windows 3.1 and Client Access for DOS with Extended Memory clients **DO NOT** use this server	
Recommended Setting:	Level 4, Log All	

Notes:

1. Levels 3 and 4 require the user to be authorized to the server function.

2. Level 4 checks SQL statements and Object/Library for authority.

3. User must have authority to SQL statement and Object/Library.

Original Virtual Print Server

Description: Original Virtual Print Server - 100

The virtual print server is used to print data from PC application programs on System i5 printers.

Where used:	Client Access for Windows 3.1 Client Access for OS/2 Client Access for DOS with Extended Memory Client Access for DOS
Server Identifier:	*VPRT
Format Name:	Always Blanks

Levels Supported:	Basic	(Levels 1,2)
	Intermediate	(Level 3)
	Advanced	(Level 4)

Limitations:	None
Recommended Setting:	Level 3 or 4, Log All

Notes:

1. At Levels 3 and 4 users must be authorized to the server function.

2. At Level 4, for each printer that is opened the user must have authority to the printer.

   *Example 1***:** To grant authority to all printers that begin with the letters PRT in library QUSRSYS enter:

Library or Folder	Object or Sub-Folder	Read
QUSRSYS	PRT*	X

Example 2: To grant authority to only the PAYROLL printer, enter:

Library or Folder	Object or Sub-Folder	Read
QUSRSYS	PAYROLL	X

Optimized Servers

This server support, provided by IBM with Client Access (now iSeries Access for Windows) beginning with OS/400 Version 3 Release 1, services optimized clients: Windows 3.1 (16 bit applications), Optimized OS/2 (32 bit applications) and Windows98, Windows 2000, Windows XP.

Additional servers are supplied by IBM for each new release of OS/400.

Central Server - Client Management

Description: Central Server - client mgmt - 100

The central server provides the ability to update the client management database on the System i5. iSeries Access for Windows uses this function when new or existing iSeries Access for Windows clients attach to the server.

Where used:	iSeries Access for Windows	
Server Identifier:	*CNTRLSRV	
Format Name:	ZSCS0100	
Levels Supported:	Basic	(Levels 1,2)
	Intermediate	(Level 3)
Limitations:	None	
Recommended Setting:	Level 1, Log All	

Notes:

1. At Level 3 users must be authorized to the server function.

2. Level 4 is not required or supported.

Central Server - Conversion Map

Description: Central Server - conversion map - 100

The central server provides support for retrieving conversion maps for clients that need them. These conversion maps are usually used on the client for ASCII to EBCDIC conversions and EBCDIC to ASCII conversions.

Where used: iSeries Access for Windows

Server Identifier: *CNTRLSRV

Format Name: ZSCN0100

Levels Supported: Basic (Levels 1,2)
Intermediate (Level 3)

Limitations: None

Recommended Setting: Level 1, Log All

Notes:

1. At Level 3 users must be authorized to the server function.

2. Level 4 is not required or supported.

Central Server - License Management

Description: Central Server - license mgmt - 100

The license management support provided by this server is very similar to the support in the original license management server for iSeries Access for Windows clients. The initial request from a client checks out a license for each iSeries Access for Windows user and the server remains active until the client is no longer communicating with the System i5.

Where used: iSeries Access for Windows

Server Identifier: *CNTRLSRV

Format Name: ZSCL0100

Levels Supported: Basic (Levels 1,2)
Intermediate (Level 3)

Limitations: None

Recommended Setting: Level 1, Log All

Notes:

1. At Level 3 users must be authorized to the server function.

2. Level 4 not required or supported.

DB2 for System i5 Database Access Request - DRDA

Description: **DRDA DB2/400 Database Access Request**

This server is used whenever a client requests a DRDA conversation connection.

Where used: Rumba Access
DB2 for System i5™
DB2 for OS/390™
DB2 Connect™

And more . . .

Server Identifier: *DRDA

Format Name: *DRDA

Levels Supported:	Basic	(Levels 1,2)
	Intermediate	(Level 3)

Limitations: None

Recommended Setting: Level 3, Log All

Notes:

1. At Levels 3 and 4 users must be authorized to the server function.

Database Server - Data Base Access - 100

Description: Database Server - data base access - 100

This server function manipulates data base files on the System i5. It allows operations to data base files, such as: create physical file, add database file member, delete file.

Where used: iSeries Access for Windows

- *Access to System i5 database through ODBC interface*
- *File transfers*

Used by ODBC*, Microsoft Access* and Microsoft Query* for object manipulation

Used by functions

Create source physical file
Create database file, based on existing file
Add, clear, delete database file member
Override database file
Delete database file override
Delete file

Server Identifier: *NDB

Format Name: ZDAD0100

Levels Supported:	Basic	(Levels 1,2)
	Intermediate	(Level 3)
	Advanced	(Level 4)

Limitations: None

Recommended Setting: Level 4, Log All

Notes:

1. At Levels 3 and 4 users must be authorized to the server function.

2. Supports generic (wildcard) object names.

Database Server - Data Base Access - 200

Description: Database Server - data base access - 200

This server function enables the addition of library list entries.

Where used:	iSeries Access for Windows for Windows95 - *Access to System i5 database through ODBC interface* - *File transfers* Used by various ODBC, DRDA™, SQL packages such as Microsoft Access, Microsoft Query, etc.
Server Identifier:	*NDB
Format Name:	ZDAD0200
Levels Supported:	Basic (Levels 1,2) Intermediate (Level 3) Advanced (Level 4)
Limitations:	- Does not support generic library names - Does not support long object names
Recommended Setting:	Level 4, Log All

Notes:

1. At Levels 3 and 4 users must be authorized to the server function.

2. At Level 4 the user must be granted authority for each library to add to the library list.

Database Server - Entry

Description: Database Server - Entry - 100

This server function is used at server initiation request. It is the request that always comes first. All other database server requests come after a request to this entry point.
This is called whenever a new connection to the database server is started and a new QZDASOINIT job is initiated to service client database requests, such as calling a stored procdure.

Where used: iSeries Access for Windows
- *Access to System i5 database through ODBC interface*
- *File transfers*

Server Identifier:	*SQL	
Format Name:	ZDAI0100	
Levels Supported:	Basic	(Levels 1,2,)
	Intermediate	(Level 3)
Limitations:	None	
Recommended Setting:	Level 3, Log All	

Notes:

1. At Level 3 users must be authorized to the server function.

2. **ALL DATABASE SERVER REQUESTS REQUIRE THIS SPECIFIC SERVER TO BE ACCESSIBLE**. A request to this server precedes all other kinds of database server requests.

3. Level 4 is not required or supported.

Database Server - Object Information - 100

Description: Database Server - object information - 100

This server function is used for requests to retrieve information about certain objects from the data base server.

Where used: iSeries Access for Windows

- *Access to System i5 database through ODBC interface*
- *File transfers*

Server Identifier: *RTVOBJINF

Format Name: ZDAR0100

Levels Supported:	Basic	(Levels 1,2)
	Intermediate	(Level 3)
	Advanced	(Level 4)

Usage: Used to retrieve information for the following objects:

- Library (or collection)
- File (or table)
- Field (or column)
- Index
- Relational database (or RDB)
- SQL package
- SQL package statement
- File member
- Record format
- Special columns

Limitations: You must restrict access to the user's default library list through user profile parameter changes or OS/400 object security.

Recommended Setting: Level 4, Log All

Notes:

1. List retrievals from *USRLIBL automatically allowed.

2. Data rights enforced.

3. At Levels 3 and 4 users must be authorized to the server function.

4. At Level 4 the user must be authorized to the OBJECT/LIBRARY.

Database Server - Object information - 200

Description: **Database Server - object information - 200**

This server function is used for requests to retrieve additional information about certain objects from the data base server, such as primary and foreign key information.

Where used: iSeries Access for Windows
- *Access to System i5 database through ODBC interface*
- *File transfers*

Server Identifier: *RTVOBJINF

Format Name: ZDAR0200

Levels Supported:	Basic	(Levels 1,2)
	Intermediate	(Level 3)

Usage: Used for requests to retrieve information for the following objects:

- Foreign keys
- Primary keys

Limitations: - You must restrict access to the user's default library list through user profile parameter changes.

Recommended Setting: Level 3, Log All

Notes:

1. At Level 3 the user must be authorized to the server function.

2. Level 4 is not required or supported.

Database Server - SQL Access

Description: **Database Server - SQL access - 100**
Database Server – SQL access – 200 (for V4R1 and above)

This server function is used when certain SQL requests are received for the data base server.

The QIBM_QZDA_SQL2 exit point takes precedence over the QIBM_QZDA_SQL1 exit point. If a program is registered for the SQL2 exit point, it will be a called, and a program for the SQL1 point will not be called.

Where used: iSeries Access for Windows

- *Access to System i5 database through ODBC interface*
- *File transfers*

Called by these functions:

ALTER TABLE
CALL
COMMENT ON
COMMIT
CREATE COLLECTION
CREATE DATABASE
CREATE INDEX
CREATE TABLE
CREATE VIEW
DELETE
DROP COLLECTION
DROP DATABASE
DROP INDEX
DROP PACKAGE
DROP TABLE
DROP VIEW
GRANT
INSERT
LABEL ON
LOCK TABLE
REVOKE
ROLLBACK
SELECT
SET TRANSACTION
UPDATE

Server Identifier: *SQLSRV

Format Name: ZDAQ0100
ZDAQ0200

Levels Supported:	Basic	(Levels 1,2)
	Intermediate	(Level 3)
	Advanced	(Level 4)

Limitations: Does not check binary field or DBPKG/DBDLIB fields.

Recommended Setting: Level 4, Log All

Notes:

1. At Levels 3 and 4 users must be authorized to the server function.

2. At Level 4 the user must be authorized to the OBJECT/LIBRARY and the SQL statement. Data authority requirements are determined by the authorized SQL statements for the user.

3. Due to a restriction within IBM's OS/400 for **versions prior to V4R1**, OS/400 delivers SQL requests to **SafeNet/400** with a limit of 512 characters in length. Since most SQL statements are normally much less than this limit, this is not a concern for most users. However, if this limit is exceeded, **SafeNet/400** will log a truncated request string into the history file. For V4R1 and above, this restriction does not apply.

   PTFs are available for earlier releases of OS/400 to enable long SQL strings. Contact IBM for details.

Data Queue Server

Description: Data Queue Server - 100

A data queue is a System i5 object that is used by System i5 application programs for communications. Applications can use data queues to pass data between jobs. Multiple System i5 jobs can send or receive data from a single data queue.

Where used:	iSeries Access for Windows	
Server Identifier:	*DATAQSRV	
Format name:	ZHQ00100	
Levels Supported:	Basic	(Levels 1,2)
	Intermediate	(Level 3)
	Advanced	(Level 4)
Limitations:	None	
Recommended Setting:	Level 1, Log All	

Notes:

1. At Levels 3 and 4 users must be granted access to the server function.

2. At Level 4 users must be granted access to specific data queues and libraries.

3. Supports generic (wildcard) data queue names. (DATAQ* = all data queue names starting with the letters DATAQ)

DHCP Address Binding Notify

Description: DHCP Address Binding Notification - 100

This server assigns IP addresses to specific client hosts.

Where used:	Any device on a TCP/IP network whenever it requests an IP address from the System i5 when the System i5 is set to be the local network DHCP server	
Server Identifier:	*DHCPB	
Format name:	DHCA0100	
Levels Supported:	Basic	(Level 1)
Limitations:	None	
Recommended Setting:	Level 1, Log All	

DHCP Address Release Notify

Description: DHCP Address Release Notification - 100

This server releases an IP address from its specific client host assignment binding.

Where used: Any device on a TCP/IP network whenever it requests an IP address from the System i5 when the System i5 is set to be the local network DHCP server

Server Identifier: *DHCPR

Format name: DHCR0100

Levels Supported: Basic (Level 1)

Limitations: None

Recommended Setting: Level 1, Log All

File Server

Description: **File Server - 100**

The file server function allows clients to store and access information, such as files and programs, on the System i5 in various formats. This server replaces the shared folder type 2 server that was used prior to Version 3 Release 1. The OS/400 file server interfaces with the integrated file system on the System i5. It provides file serving capabilities equivalent to shared folders, but also allows clients to access information in any of the new file systems within OS/400.

Where used: iSeries Access for Windows
- *Access to entire file system*
- *Windows Explorer and other applications*

Server Identifier: *FILESRV

Format Name: PWFS0100

Levels Supported:	Basic	(Levels 1,2)
	Intermediate	(Level 3)
	Advanced	(Level 4)

Limitations:
- Directory structure has a maximum of 20 deep
- Does not differentiate between upper and lower case file names
- Does not support long file names. Names over 10 characters are truncated
- Allows setting of global authority to IBM supplied folders and file systems
- Authority is granted to a folder and all data that it contains. Different object/file authorities within the same folder is not available.

Recommended Setting: Level 4, Log All

Notes:

1. When set to Levels 3 or 4, each iSeries Access for Windows user must be specifically authorized to this server to access their shared folder and update functions.

2. To grant authority to all folders and all file systems use:

Library	Object
or Folder	or Sub-Folder
*ALLFLR	*ALL

To enter *ALLFLR/ *ALL you must be signed on as QSECOFR.

Proper Data Rights must be selected also.

3. At Level 4, to authorize a user for access to a non-IBM folder within the QDLS file system (shared folders), you must enter two records in the OBJECT/USER security file.

Example 1: A user requires access to a folder called PERSONNEL within QDLS.

Network Request: /QDLS/PERSONNEL

Entries Required:

	Library or Folder	Object or Sub-Folder	Read
Entry #1	QDLS	PERSONNEL	X
Entry #2	PERSONNEL	*ALL	X

Example 2: You can add specific folder names in place of *ALL to further extend the directory path.

Network Request: /QDLS/PERSONNEL/PAYROLL/SALARY

Entries Required:

	Library or Folder	Object or Sub-Folder	Read
Entry #1	QDLS	PERSONNEL	X
Entry #2	PERSONNEL	*ALL	X
Entry #3	PAYROLL	SALARY	X
Entry #4	SALARY	*ALL	X

4. This is a typical iSeries Access for Windows user security set up if automatic read to IBM folders is not enabled (found on Special Jobs Menu, Option 2):

Library or Folder	Object or Sub-Folder	Read
QDLS	QIWSFLR	X
QIWSFLR	*ALL	X

5. **SafeNet/400** does not support the full long file names or lower case names, SafeNet/400 will truncate each request to a maximum of 10 characters. To allow access to file

systems **Qopensys, Qfilesys.400 and home**, key in the first 10 positions of each file system name only.

Example:

Network Request: /Qfilesys.400/QSYS.LIB/PAYROLL.LIB/SALARY.FIL

Entries Required:

	Library or Folder	Object or Sub-Folder	Read
Entry #1	QFILESYS.4	QSYS.LIB	X
Entry #2	QSYSLIB	PAYROLL.LI	X
Entry #3	PAYROLL.LI	SALARY.FIL	X

SafeNet/400 will convert all requests to uppercase, then check the first ten characters in each directory name for a match.

Note: When native libraries or objects are accessed via the file server, .LIB, .file, etc. are added to the end of the name. You must enter the .LIB or .file in the user to object control file. If the same user accesses these same objects through another server also, (SQL, for example) you must also enter the authorities without the .LIB and .file.

Example:

For the path through the file server: home/TEST.LIB/abc.file you must enter:

Library	Object	Auth
home	TEST.LIB	X
TEST.LIB	*ALL	X

For SQL or other access you also need:

Library	Object	Auth
TEST	*ALL	X

FTP Client Request Validation

Description: **FTP Client Request Validation**

This function is used whenever the System i5 is a client, issuing FTP commands to a remote system.

Where used:	System i5 command lines, interactive and batch jobs can initiate an FTP client request
Server Identifier:	*FTPClient
Format Name:	VLRQ0100

Levels Supported:	Basic	(Level 1,2)
	Intermediate	(Level 3)
	Advanced	(Level 4)

Usage Notes/Limitations:

At Level 3 or Level 4 you can implement IP address controls. This will allow you to limit what target addresses/systems an FTP client can connect to. See commands:

```
CHGFTPSET IPCTLC(*YES) and WRKTCPIPA *FTPCLIENT
```

You can also review ‘Setting up TCP/IP Address Controls’ in Chapter 3 of this guide.

Recommended Setting: Level 4, Log All

Important Note:

When the FTP Client point is set to Level 4, only the GET and PUT FTP sub-commands are required. The other commands, when using the FTP Client, are for the TARGET SYSTEM ONLY (sent to/run on the target system).

When authorizing users to the GET/PUT sub-commands, the assumed object authority is reversed from authorities required for the FTP Server point and the same objects.

See the following examples.

Using FTP Client:

- Sending an object to a remote system
  An FTP PUT of object ABC in an FTP Client session requires *READ authority to object ABC on the local machine.
- Get an object from a remote system
  An FTP GET of object ABC in an FTP Client session requires *OBJMGT authority to the object ABC on the local machine.

Using FTP Server:

- Send an object to local system
  An FTP PUT of object ABC in an FTP Server session requires *OBJMGT authority to the object ABC on the LOCAL machine.
- Get an object from the local system
  An FTP GET of object ABC in an FTP Server session requires *READ authority to the object ABC on the LOCAL machine.

FTP Logon Server

Description: FTP Logon Server 1 - 100

This server is used any time the System i5 answers an FTP start request from another system or user. It is available in OS/400 versions V3R7 through V4R1

Where used:	Internets and Intranets MS Windows DOS And most other operating systems	
Server Identifier:	*FTPLOGON	
Format Name:	TCPL0100	
Levels Supported:	Basic	(Level 1,2)
	Intermediate	(Level 3)
Limitations:	None	
Recommended Setting:	Level 3, Log All	

FTP Logon Server

Description: FTP Logon Server 2 - 200

This server is used any time the System i5 answers an FTP start request from another system or user. It is available in OS/400 versions V4R2 and above.

Where used:	Internets and Intranets MS Windows DOS And most other operating systems	
Server Identifier:	*FTPLOGON2	
Format Name:	TCPL0200	
Levels Supported:	Basic	(Level 1,2)
	Intermediate	(Level 3)
Limitations:	None	
Recommended Setting:	Level 3, Log All	

FTP Logon Server

Description: FTP Logon Server 3 – 300

This server is used any time the System i5 answers an FTP start request from another system or user. It is available in OS/400 versions V5R1 or above.

Where used:	Internets and Intranets MS Windows DOS And most other operating systems	
Server Identifier:	*FTPLOGON3	
Format Name:	TCPL0300	
Levels Supported:	Basic	(Level 1,2)
	Intermediate	(Level 3)
Limitations:	None	
Recommended Setting:	Level 3, Log All	

FTP Server Request Validation

Description: FTP Server Request Validation

This function is used whenever the System i5 receives an FTP command it must act upon.

Where used:	Internets and Intranets MS Windows And most other operating systems	
Server Identifier:	*FTPSERVER	
Format Name:	VLRQ0100	
Levels Supported:	Basic	(Level 1,2)
	Intermediate	(Level 3)
	Advanced	(Level 4)
Limitations:	None	
Recommended Setting:	Level 4, Log All	

Notes:

1. At Level 4, users must be authorized to the objects and the FTP statements they require and the CL commands they may issue to the System i5.

3. Only at Level 4 are 'ANONYMOUS' logons allowed. This is in conjunction with the special FTP security settings. See Chapter 4 in this guide, 'Setting up FTP' (**CHGFTPSET** command).

4. You can limit FTP connections from specific IP Addresses. See commands:

   ```
   CHGFTPSET IPCTL(*YES) and   WRKTCPIPA *FTPSERVER
   ```

   You can also review 'Setting up TCP/IP Address Controls' in Chapter 3 of this guide.

Network Print Server - Entry

Description: Network Print Server - entry - 100

This server function is used when the network print server is started.

Where used:	iSeries Access for Windows	
Server Identifier:	QNPSERVR	
Format Name:	ENTR0100	
Levels Supported:	Basic Intermediate	(Levels 1,2) (Level 3)
Limitations:	None	
Recommended Setting:	Level 3, Log All	

Notes:

1. At Level 3 users must be granted access to the server function.

2. Level 4 is not required or supported.

Network Printer Server - Spool File

Description: Network Print Server - spool file - 100

This server function is used after the network print server receives a request to process an existing spooled output file.

Where used:	iSeries Access for Windows	
Server Identifier:	QNPSERVR	
Format Name:	SPLF0100	
Levels Supported:	Basic	(Levels 1,2)
	Intermediate	(Level 3)
	Advanced	(Level 4)
Limitations:	Level 4 grants spool file management rights to the owner of the spool file only.	
Recommended Setting:	Level 4, Log All	

Notes:

1. At Levels 3 and 4 users must be granted access to the server function.

2. Level 4 requires no special set up. (see Limitations above)

3. No specific object authorizations required.

Pre-Power Down

Description: Pre-Power Down Server

This program is called whenever the PWRDWNSYS or ENDSYS command is issued

Where used: Any interface, command line or program that can issue the PWRDWNSYS or ENDSYS command

Server Identifier: PWRDWN

Format Name: PWRD0100

Levels Supported: Basic (Level 1)

Limitations: None

Recommended Setting: Level 1

Notes:

1. To use the pre-power down program call, create a CL program called PWRDWNCL.

Remote Command and Distributed Program Call Server

Description: Remote Command/Program Call - 100

The remote command and distributed program call server is provided to allow client users and applications to issue System i5 CL commands and call programs.

Where used: iSeries Access for Windows

Server Identifier: *RMTSRV

Format Name: CZRC0100

Levels Supported:

Basic	(Levels 1,2)
Intermediate	(Level 3)
Advanced	(Level 4)

And special global control setting

Limitations: Cannot check Library/Object security on imbedded command strings

Recommended Setting: Level 4, Log All

Notes:

1. For X-1002 Remote Command Call, the same rules apply here as for *DDM commands. You must use the Special Jobs Menu to allow or reject remote commands entering via this server. In addition, see Note 3 below.

   One setting controls both *RMTSRV X-1002 and *DDM command servers.

2. Used by Operations Navigator for system object access.

   Each GUI request from system object access triggers a program call. Most are in QUSRSYS or QGY libraries. By allowing QGY/*ALL and QUSRSYS/*ALL Read Data Rights, you let users access GUI interfaces.

3. At Level 4 you must authorize each user to the CL commands they may issue through this server.

REXEC Logon Server

Description: REXEC Logon Server 1 - 100

This server is used to validate a client request to start the REXEC Server. It is available in all versions of OS/400.

Where used: Windows and OS/2 Desktop Add-in Applications
Other Clients using REXEC Applications

Server Identifier: *REXLOGON

Format name: TCPL0100

Levels Supported:	Basic	(Levels 1,2)
	Intermediate	(Level 3)

Limitations: None

Recommended Setting: Level 3, Log All

Usage Notes:

You can limit FTP connections from specific IP Addresses. See commands:

```
CHGFTPSET IPCTL(*YES) and WRKTCPIPA *FTPSERVER
```

You can also review ‘Setting up TCP/IP Address Controls’ in Chapter 3 of this guide.

REXEC Logon Server

Description: REXEC Logon Server 2 - 200

This server is used to validate a client request to start the REXEC Server. It is available in OS/400 versions V5R1 and above.

Where used:	Windows and OS/2 Desktop Add-in Applications Other Clients using REXEC Applications	
Server Identifier:	*REXLOGON2	
Format name:	TCPL0300	
Levels Supported:	Basic	(Levels 1,2)
	Intermediate	(Level 3)
Limitations:	None	
Recommended Setting:	Level 3, Log All	

Usage Notes:

You can limit FTP connections from specific IP Addresses. See commands:

```
CHGFTPSET IPCTL(*YES) and WRKTCPIPA *FTPSERVER
```

You can also review ‘Setting up TCP/IP Address Controls’ in Chapter 3 of this guide.

REXEC Request Validation Server

Description: REXEC Request Validation Server

This server is initiated whenever a client issues a REX statement to the System i5.

Where used:	Windows and OS/2 Desktop Add-in Applications Other Clients using REXEC Applications	
Server Identifier:	*REXSERVER	
Format name:	VLRQ0100	
Levels Supported:	Basic	(Levels 1,2)
	Intermediate	(Level 3)
	Advanced	(Level 4)
Limitations:	None	
Recommended Setting:	Level 3, Log All	

Usage Notes:

You can limit FTP connections from specific IP Addresses. See commands:

```
CHGFTPSET IPCTL(*YES) and WRKTCPIPA *FTPSERVER
```

You can also review 'Setting up TCP/IP Address Controls' in Chapter 3 of this guide.

ShowCase Strategy Validation Server**

Description: Showcase Strategy Validation Server

This server is initiated by a client utilizing the Showcase Strategy** product with the proper exit point added to OS/400.

Please follow the instructions from Showcase to properly register the ShowCase Exit Program. You MAY have to use the ADDEXITPGM command to add the exit point for ShowCase to your System i5 Server.

Where used:	Any client utilizing Showcase Strategy** Application	
Server Identifier:	*SHOWCASE	
Format name:	SRCS0100	
Levels Supported:	Basic	(Levels 1,2)
	Intermediate	(Level 3)
	Advanced	(Level 4)
Limitations:	None	
Recommended Setting:	Level 4, Log All	

<u>Important Notes on setting up a user for ShowCase** Strategy</u>**

Although Showcase uses SQL statements to access OS/400 data, SafeNet/400 does NOT verify the SQL statement authority. SafeNet/400 ONLY verifies the user to server and user to objects. The SQL Statement is NOT interrogated for authority. If the user issues a SELECT statement, the object authority required is *READ. If the user issues a DELETE statement, data *DELETE authority is required.

You DO NOT have to set up SQL statement authority for the Showcase Strategy** users.

TCP Signon Server

Description: TCP Signon Server - 100

The signon server provides security for clients that use TCP/IP communications support. This security function prevents access to the System i5 for users with expired passwords or allows entry to only specific users.

Where used:	iSeries Access for Windows	
Server Identifier:	*SIGNON	
Format Name:	ZSOY0100	
Levels Supported:	Basic	(Level 1,2)
	Intermediate	(Level 3)
Limitations:	None	
Recommended Setting:	Level 1, Log All	

Notes:

1. Level 3 requires specific authority to the server function.

2. Level 4 is not required or supported.

TELNET Device Initialization
TELNET Device Termination

Description: TELNET Device Initialization - *TELNETON
TELNET Device Termination - *TELNETOFF

The TELNET servers provide for security when using TCP/IP and TELNET clients. This point allows the restriction by IP address and password type. Auto-signon can also be configured. TELNET Device Termination allows for session logging and device management upon session termination. *TELNETOFF is dependent upon the setting of *TELNETON.

Where used: Any TN5250 (TELNET client)
MS Windows
iSeries Access for Windows

Server Identifier: *TELNETON
*TELNETOFF

Format Name: INIT0100
TERM0100

Levels Supported:	Basic	(Level 1,2)
	Intermediate	(Level 3)

Limitations: See Chapter 3 in this guide, ‘TELNET, TCP/IP Address Controls’

Recommended Setting: Level 3, Log All

Notes:

1. Level 3 requires correct IP addressing in control file (WRKTCPIPA *TELNET)

2. You can limit FTP connections from specific IP Addresses. See commands:

   CHGFTPSET IPCTL(*YES) and WRKTCPIPA *FTPSERVER

   You can also review ‘Setting up TCP/IP Address Controls’ in Chapter 3 of this guide.

TFTP Server Request Validation

Description: TFTP Server Request Validation

Clients utilizing TFTP (Trivial File Transfer Protocol), such as the IBM Net Station use this server.

Where used:	IBM Net Station Boot	
Server Identifier:	*TFTPSRVR	
Format name:	VLRQ0100	
Levels Supported:	Basic	(Levels 1,2)
	Intermediate	(Level 3)
Limitations:	None	
Recommended Setting:	Level 3, Log All	

User Profile Servers

Description: **Add User Profile**
Change User Profile
Delete User Profile
Restore User Profile

These servers are called each time a user profile command is issued.

Where used: Any interface or command line that can issue a user profile associated OS/400 command

Server Identifier:	**Format:**
*CHGPRF	CHGP0100
*CRTPRF	CRTP0100
*DLTPRFA	DLTP0100
*DLTPRFB	DLTP0200
*RSTPRF	RSTP0100

Levels Supported: Basic (Levels 1)

Limitations: None

Recommended Setting: Level 1, Log All

Notes:

1. This point simply logs which user profile was affected, who performed the action, and when it was done.

INDEX